# Formalized Timed Automata

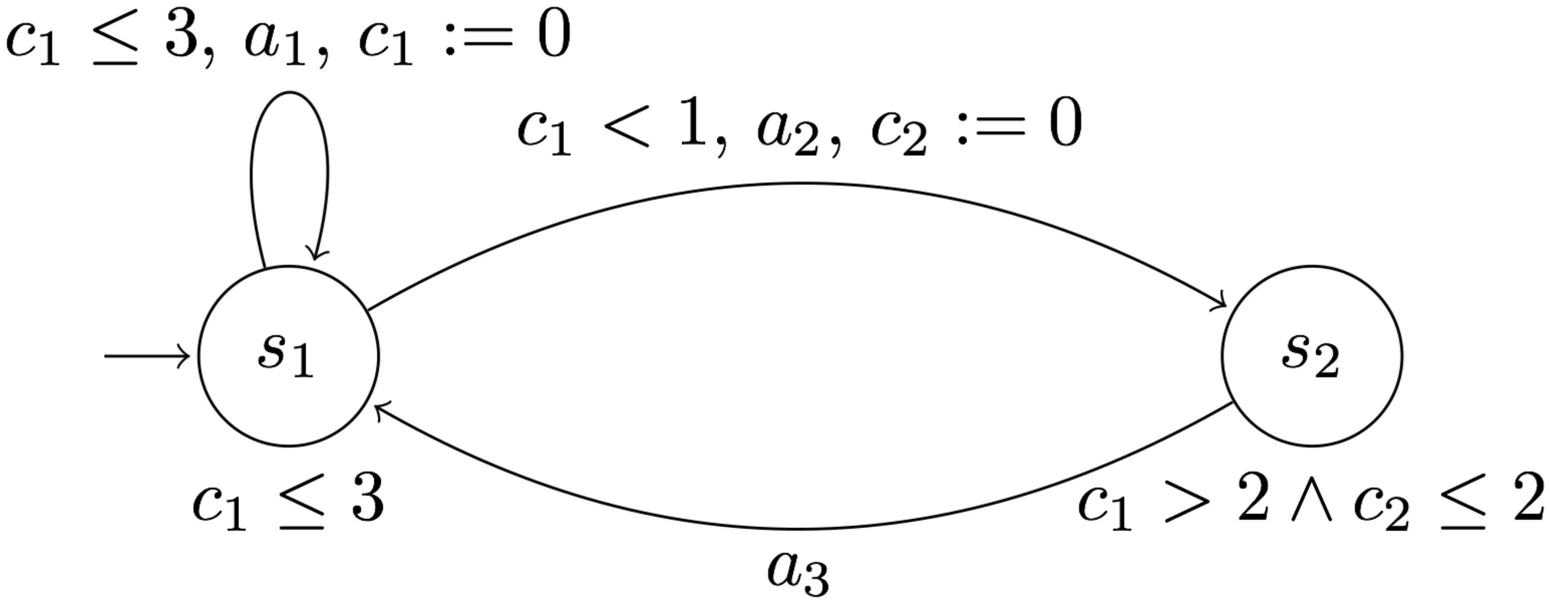
Simon Wimmer

Fakultät für Informatik, Technische Universität München

ITP Talk on August 24, 2016

# Timed Automata

- Timed Automata (TA) ≈ Finite Automata with clocks
  - Clock guards on transitions and clock invariants on locations
  - Transitions can reset clocks



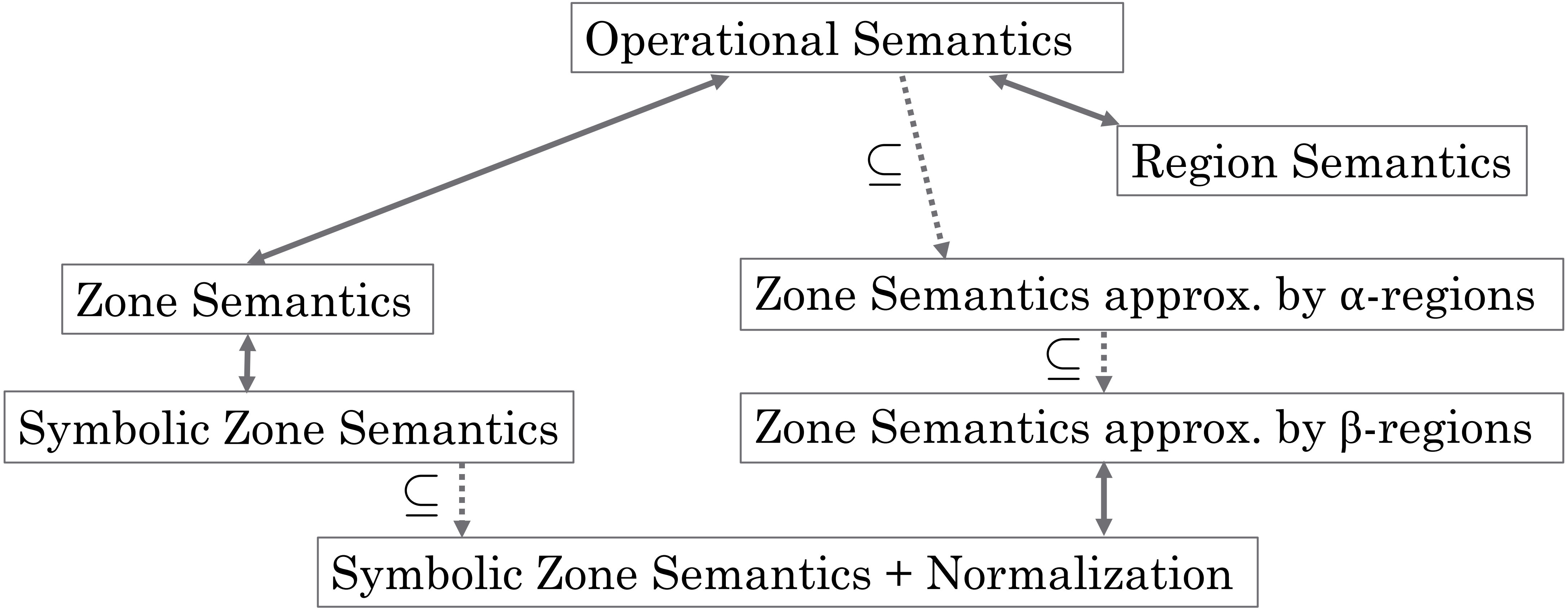
# Timed Automata (2)

- Model Checking: PSPACE
  - Initial decidability from the region construction of Alur & Dill
  - Practical tools (UPPAAL): symbolic forward reachability algorithm
- Bouyer: forward reachability analysis not correct for general TA
  - However, correctness given for the class of diagonal-free TA
- This formalization: formalization of TA basics and symbolic forward reachability analysis in Isabelle/HOL
  - Region construction as a reasoning tool

# This Formalization

- Formalization of TA basics and forward reachability analysis
- Region construction for decidability and as a reasoning tool
- Symbolic analysis with Difference Bound Matrices (DBMs)
- Correctness of approximation operation forward reachability analysis (Bouyer)

# Semantics Zoo




Given start state $(l, u)$ and destination $l'$, is there a run $A \vdash (l, u) \rightarrow^* (l', u')$ for some $u'$?

# Formalization – Clock Constraints

$$\textbf{datatype}\ ('c,\ 't)\ \mathit{cconstraint} =$$
$$\mathit{AND}\ (('c,\ 't)\ \mathit{cconstraint})\ (('c,\ 't)\ \mathit{cconstraint})\ |$$
$$\mathit{LT}\ 'c\ 't\ |\ \mathit{LE}\ 'c\ 't\ |\ \mathit{EQ}\ 'c\ 't\ |\ \mathit{GT}\ 'c\ 't\ |\ \mathit{GE}\ 'c\ 't$$

represents $c \sim d$ for $\sim = <, \leq, =, >, \geq$ .

Diagonal-free TA: No constraints of the form $c_1 - c_2 \sim d$ .

# Formalization – Clock Constraints

$$\textbf{datatype}\ ('c,\ 't)\ \mathit{cconstraint} =$$
$$\mathit{AND}\ (('c,\ 't)\ \mathit{cconstraint})\ (('c,\ 't)\ \mathit{cconstraint})\ |$$
$$\mathit{LT}\ 'c\ 't\ |\ \mathit{LE}\ 'c\ 't\ |\ \mathit{EQ}\ 'c\ 't\ |\ \mathit{GT}\ 'c\ 't\ |\ \mathit{GE}\ 'c\ 't$$

represents $c \sim d$ for $\sim = <, \leq, =, >, \geq$ .

# Formalization – Clock Constraints

**datatype** $('c,\ 't)\ \mathit{cconstraint} =$
$\mathit{AND}\ ((('c,\ 't)\ \mathit{cconstraint})\ (('c,\ 't)\ \mathit{cconstraint})\ |$
$\mathit{LT}\ 'c\ 't\ |\ \mathit{LE}\ 'c\ 't\ |\ \mathit{EQ}\ 'c\ 't\ |\ \mathit{GT}\ 'c\ 't\ |\ \mathit{GE}\ 'c\ 't$

represents $c \sim d$ for $\sim \quad \in \quad <, \leq, =, \geq, >.$

# Formalization – Timed Automata

- Timed Automaton $\mathcal{A} = (\mathcal{T}, \mathcal{I})$
  - $I ::\ 's \Rightarrow ('c,\ 't)\ cconstraint$
  - $\mathcal{T}$ a set of transitions of the form $A \vdash l \longrightarrow^{g,a,r} l'$
    - $l ::\ 's$ start location
    - $l' ::\ 's$ end location
    - $a ::\ 'a$ action label
    - $g :: ('c,\ 't)\ cconstraint$ guard
    - $r ::\ 'c\ list$ clocks to reset

# Operational Semantics

- Valuations $u :: {'c} \Rightarrow {'t}$ Time lapse: $u \oplus d = (\lambda x.\ u\ x + d)$
- States $(l, u)$
- Constraint satisfaction

$$u \vdash \mathit{AND}\ (\mathit{LT}\ c_1\ \mathit{1})\ (\mathit{EQ}\ c_2\ \mathit{2}) \text{ if } u\ c_1 < 1 \text{ and } u\ c_2 = 2$$

- Delay steps $\dfrac{u \vdash \mathit{inv\text{-}of}\ A\ l \land u \oplus d \vdash \mathit{inv\text{-}of}\ A\ l \land \mathit{0} \le d}{A \vdash \langle l,\ u\rangle \rightarrow^{d} \langle l,\ u \oplus d\rangle}$
- Action steps

$$\frac{A \vdash l \longrightarrow^{g,a,r} l' \land u \vdash g \land u' \vdash \mathit{inv\text{-}of}\ A\ l' \land u' = [r \rightarrow \mathit{0}]u}{A \vdash \langle l,\ u\rangle \rightarrow_a \langle l',\ u'\rangle}$$

# Operational Semantics

- Valuations $u :: {}'c \Rightarrow {}'t$  Time lapse: $u \oplus d = (\lambda x.\ u\ x + d)$
- States $(l, u)$
- Constraint satisfaction

$$u \vdash \mathit{AND}\ (\mathit{LT}\ c_1\ \mathit{1})\ (\mathit{EQ}\ c_2\ \mathit{2}) \text{ if } u\ c_1 < 1 \text{ and } u\ c_2 = 2$$

- Delay steps

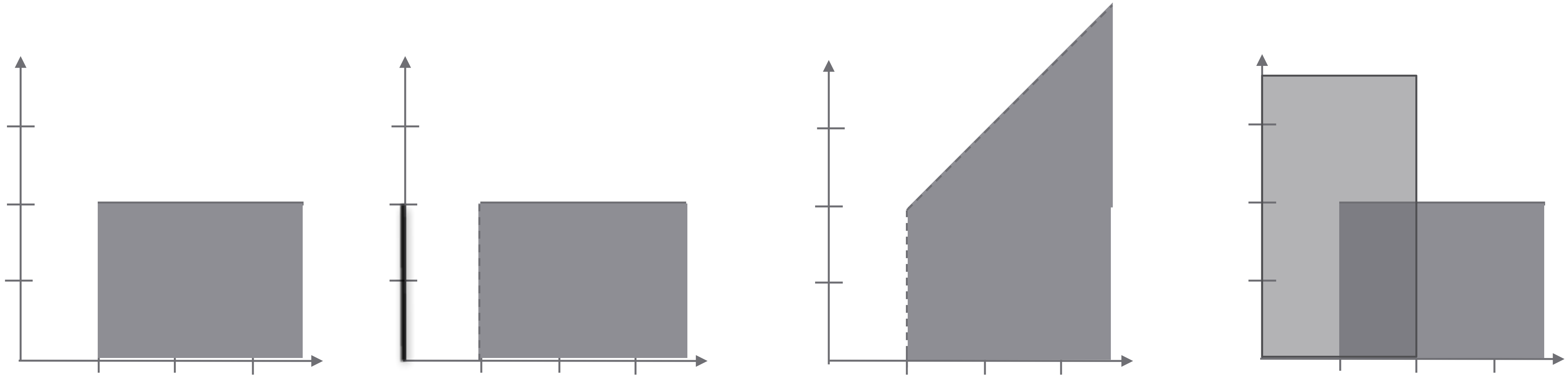
$$\frac{u \vdash I(l) \qquad u \oplus d \vdash I(l) \qquad 0 \leq d}{A \vdash \langle l, u \rangle \to \langle l, u \oplus d \rangle}$$

- Action steps

$$\frac{A \vdash l \longrightarrow^{g,a,r} l' \qquad u \vdash g \qquad u' \vdash I(l') \qquad u' = [r \to 0]u}{A \vdash \langle l, u \rangle \to \langle l', u' \rangle}$$

# Zone Semantics

- First abstraction: Zones $Z :: ('c \Rightarrow 't)\, set$
  - Convex sets of valuations, i.e. a set of valuations satisfying a clock constraint
- Operations on zones



$Z =$ $\{u \mid u\, c_1 > 1 \wedge u\, c_2 \leq 2\}$

$Z_{c_2 \to 0} =$ $\{u \mid u\, c_1 = 0 \wedge u\, c_2 \leq 2\}$

$Z^{\uparrow} =$ $\{u \mid u\, c_1 > 1 \wedge u\, c_2 - u\, c_1 < 1\}$

$Z \cap \{u \mid u\, c_1 \leq 2\}$

# Zone Semantics

- First abstraction: Zones $Z :: ('c \Rightarrow 't)\, set$
  - Convex sets of valuations, i.e. a set of valuations satisfying a clock constraint
  - Delay: $Z^{\uparrow} = \{u \oplus d \mid u \in Z \wedge 0 \leq d\}$ Reset: $Z_{r \rightarrow 0} = \{[r \rightarrow 0]u \mid u \in Z\}$
  - Semantics

$$\frac{}{A \vdash \langle l,\, Z\rangle \rightsquigarrow \langle l,\, (Z \cap \{u \mid u \vdash \mathit{inv\text{-}of}\ A\ l\})^{\uparrow} \cap \{u \mid u \vdash \mathit{inv\text{-}of}\ A\ l\}\rangle}$$

$$\frac{A \vdash l \longrightarrow^{g,a,r} l'}{A \vdash \langle l,\, Z\rangle \rightsquigarrow \langle l',\, (Z \cap \{u \mid u \vdash g\})_{r \rightarrow 0} \cap \{u \mid u \vdash \mathit{inv\text{-}of}\ A\ l'\}\rangle}$$

  - Sound and complete w.r.t. reachability

# Zone Semantics

- First abstraction: Zones $Z :: ('c \Rightarrow 't)\ set$
  - Delay: $Z^{\uparrow} = \{u \oplus d \mid u \in Z \wedge 0 \leq d\}$ Reset: $Z_{r \rightarrow 0} = \{[r \rightarrow 0]u \mid u \in Z\}$
  - Semantics

$$\frac{}{A \vdash \langle l,\ Z\rangle \rightsquigarrow \langle l,\ (Z \cap \{u \mid u \vdash \textit{inv-of}\ A\ l\})^{\uparrow} \cap \{u \mid u \vdash \textit{inv-of}\ A\ l\}\rangle}$$

$$\frac{A \vdash l \longrightarrow^{g,a,r} l'}{A \vdash \langle l,\ Z\rangle \rightsquigarrow \langle l',\ (Z \cap \{u \mid u \vdash g\})_{r \rightarrow 0} \cap \{u \mid u \vdash \textit{inv-of}\ A\ l'\}\rangle}$$

  - Compare

$$\frac{u \vdash I(l) \qquad u \oplus d \vdash I(l) \qquad 0 \leq d}{A \vdash \langle l, u\rangle \rightarrow \langle l, u \oplus d\rangle}$$

$$\frac{A \vdash l \longrightarrow^{g,a,r} l' \qquad u \vdash g \qquad u' \vdash I(l) \qquad u' = [r \rightarrow 0]u}{A \vdash \langle l, u\rangle \rightarrow \langle l', u'\rangle}$$

  - Sound and complete w.r.t. reachability

# Zone Semantics

- First abstraction: Zones $Z :: ('c \Rightarrow 't)\, set$
  - Delay: $Z^{\uparrow} = \{u \oplus d \mid u \in Z \wedge 0 \leq d\}$ Reset: $Z_{r \to 0} = \{[r \to 0]u \mid u \in Z\}$
  - Semantics

$$\frac{}{A \vdash \langle l, Z \rangle \rightsquigarrow \langle l, (Z \cap \{u \mid u \vdash I(l)\})^{\uparrow} \cap \{u \mid u \vdash I(l)\} \rangle}$$

$$\frac{A \vdash l \longrightarrow^{g,a,r} l'}{A \vdash \langle l, Z \rangle \rightsquigarrow \langle l', (Z \cap \{u \mid u \vdash g\})_{r \to 0} \cap \{u \mid u \vdash I(l')\} \rangle}$$

  - Compare

$$\frac{u \vdash I(l) \qquad u \oplus d \vdash I(l) \qquad 0 \leq d}{A \vdash \langle l, u \rangle \to \langle l, u \oplus d \rangle}$$

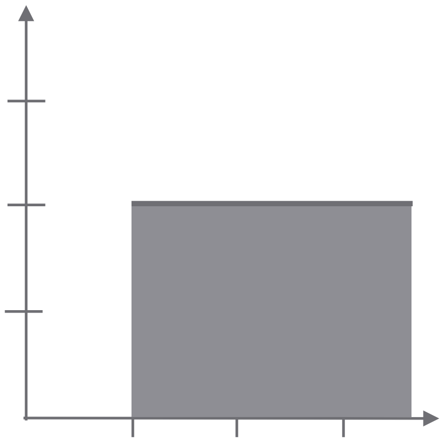
$$\frac{A \vdash l \longrightarrow^{g,a,r} l' \qquad u \vdash g \qquad u' \vdash I(l) \qquad u' = [r \to 0]u}{A \vdash \langle l, u \rangle \to \langle l', u' \rangle}$$

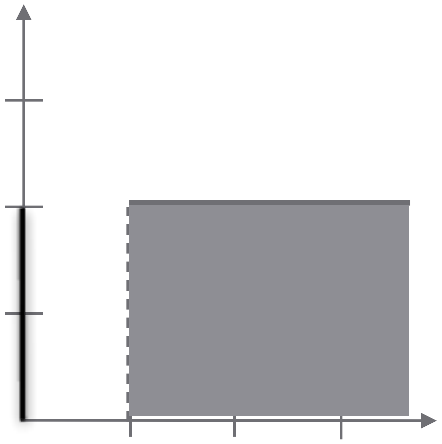
  - Sound and complete w.r.t. reachability

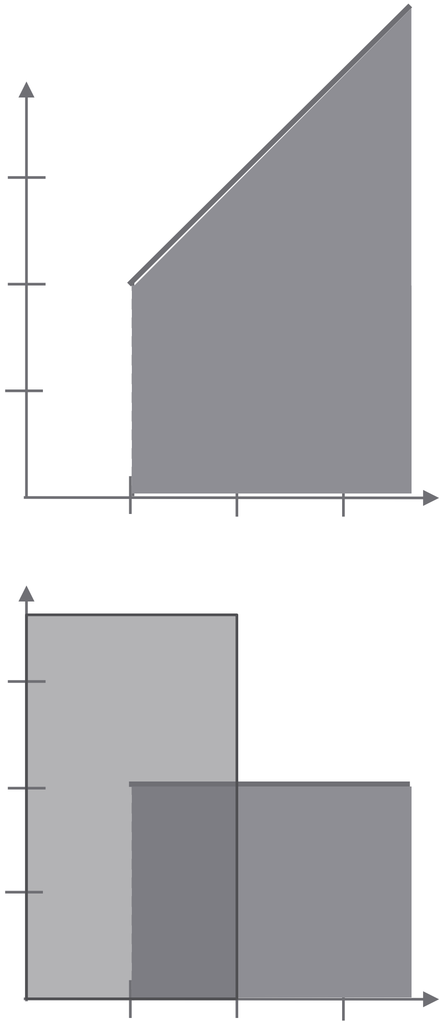
# Difference Bound Matrices

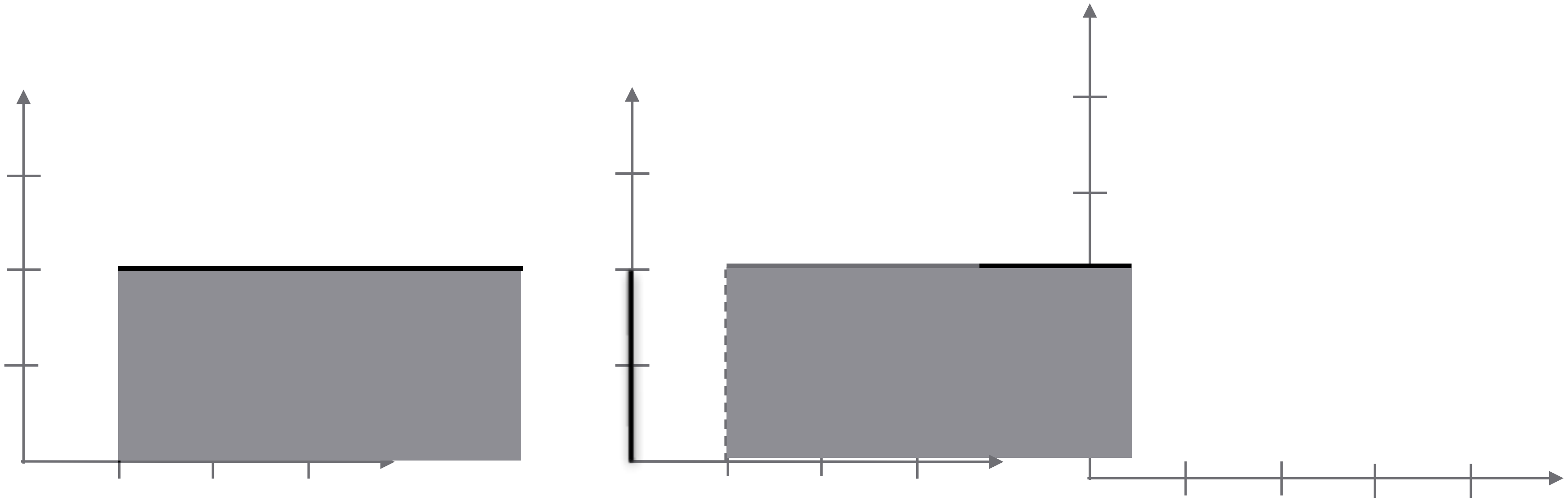
- DBMs: symbolic representation of zones
  - Rows and columns: clocks
  - Entries: difference constraints between clocks
  - $\mathbf{datatype}\ {}'t\ \mathit{DBMEntry} = \mathit{Le}\ {}'t \mid \mathit{Lt}\ {}'t \mid \infty$
  - ${}'t\ \mathit{DBM} \equiv \mathit{nat} \Rightarrow \mathit{nat} \Rightarrow {}'t\ \mathit{DBMEntry}$
  - Artificial zero clock (**0**) for bounds on individual clocks
- Example: zone with $c_1 > \mathit{3}$ and $c_2 \leq \mathit{4}$

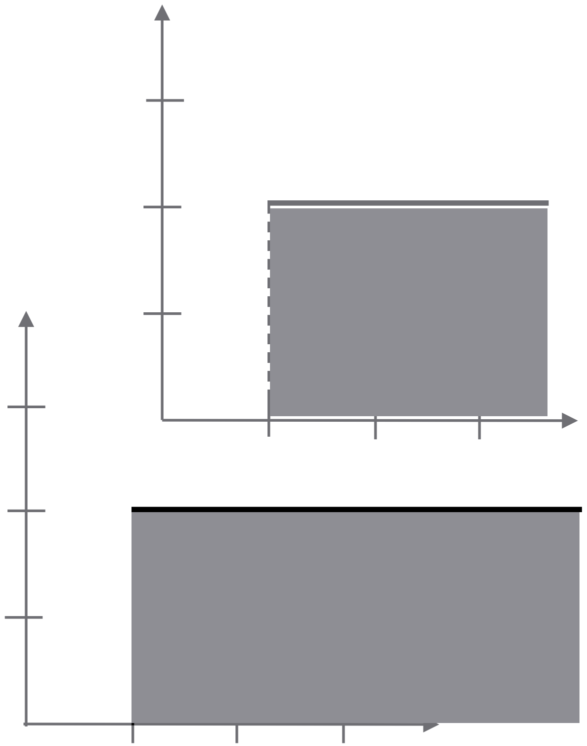
$$\begin{array}{c|ccc} & \mathbf{0} & c_1 & c_2 \\ \hline \mathbf{0} & \infty & \mathit{Lt}\ (-\mathit{3}) & \mathit{Le}\ \mathit{0} \\ c_1 & \infty & \infty & \infty \\ c_2 & \mathit{Le}\ \mathit{4} & \infty & \infty \end{array} \qquad \begin{array}{c|ccc} & \mathbf{0} & c_1 & c_2 \\ \hline \mathbf{0} & \mathit{Le}\ \mathit{0} & \mathit{Lt}\ (-\mathit{3}) & \mathit{Le}\ \mathit{0} \\ c_1 & \infty & \mathit{Le}\ \mathit{0} & \infty \\ c_2 & \mathit{Le}\ \mathit{4} & \mathit{Lt}\ \mathit{1} & \mathit{Le}\ \mathit{0} \end{array}$$

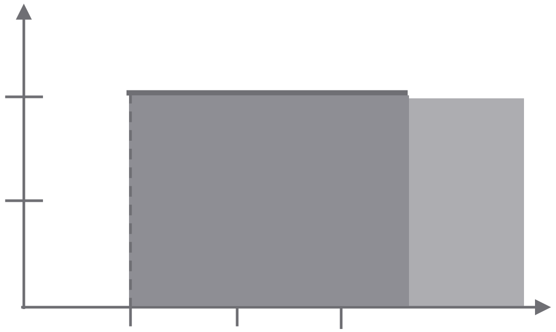












# Arithmetic on DBM entries

- Orderings $\prec$ and $\preceq$

$$\frac{a < b}{Le\ a \prec Le\ b} \quad \frac{a < b}{Le\ a \prec Lt\ b} \quad \frac{a < b}{Lt\ a \prec Lt\ b} \quad \frac{a \leq b}{Lt\ a \prec Le\ b} \quad \frac{}{Lt\ \_ \prec \infty} \quad \frac{}{Le\ \_ \prec \infty}$$

- $\forall\, i\ j.\ i \leq n \longrightarrow j \leq n \longrightarrow M\ i\ j \preceq M'\ i\ j \Longrightarrow [M]_{v,n} \subseteq [M']_{v,n}$
- Addition: $a \boxplus \infty,\ \infty \boxplus b,\ Le\,3 \boxplus Lt\,(-2) = Lt\,(-1)$
- Length of paths

# Arithmetic on DBM entries

- Addition: $a \boxplus \infty,\ \infty \boxplus b,\ Le\,3 \boxplus Lt\,(-2) = Lt\,(-1)$
- Orderings $\prec$ and $\preceq$
  - $Lt\,0 \preceq Le\,0,\ Le\,0 \preceq Lt\,1,\ Lt\,1 \prec \infty$
  - $\forall\, i\ j.\ i \le n \longrightarrow j \le n \longrightarrow M\ i\ j \preceq M'\ i\ j \Longrightarrow [M]_{v,n} \subseteq [M']_{v,n}$
- Length of paths
  - $len\ M\ s\ t\ [] = M\ s\ t \qquad len\ M\ s\ t\ (w \cdot ws) = M\ s\ w \boxplus len\ M\ w\ t\ ws$
  - $Lt\ (u\ i\ -\ u\ j) \prec len\ M\ i\ j\ xs$ if $u \in [M]_{v,n}$
- Negative Cycles:

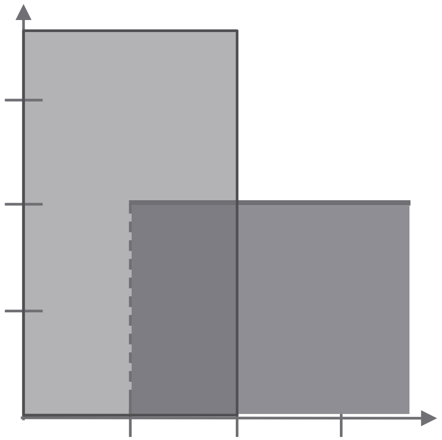
$$\begin{array}{cc} & \begin{array}{ccc} \mathbf{0} & c_1 & c_2 \end{array} \\ \begin{array}{c} \mathbf{0} \\ c_1 \\ c_2 \end{array} & \begin{pmatrix} \infty & Le\ 0 & Le\ 0 \\ \infty & \infty & Lt\ (-3) \\ \infty & Le\ 3 & Le\ 0 \end{pmatrix} \end{array}$$

# Arithmetic on DBM entries

- Addition: $a \boxplus \infty = \infty, Le\ 3 \boxplus Lt\ (-2) = Lt\ 1$
- Orderings $\prec$ and $\preceq$
  - $Lt\, 0 \preceq Le\, 0,\ Le\, 0 \preceq Lt\, 1,\ Lt\, 1 \prec \infty$
  - $\forall\, i\ j.\ i \le n \longrightarrow j \le n \longrightarrow M\ i\ j \preceq M'\ i\ j \Longrightarrow [M]_{v,n} \subseteq [M']_{v,n}$
- Length of paths
  - $len\ M\ s\ t\ [] = M\ s\ t \qquad len\ M\ s\ t\ (w \cdot ws) = M\ s\ w \boxplus len\ M\ w\ t\ ws$
  - $Lt\ (u\ i - u\ j) \prec len\ M\ i\ j\ xs$ if $u \in [M]_{v,n}$

# DBM Operations

- Intersection $A \sqcap B = (\lambda\, i\, j.\, min\, (A\, i\, j)\, (B\, i\, j))$
  - Correctness: $[A]_{v,n} \cap [B]_{v,n} = [A \sqcap B]_{v,n}$



- Similarly reset, delay and intersection with clock constraints

# DBM Operations (2)

- Floyd-Warshall algorithm
  - Computes canonical form:
    $\forall\, i\ j\ k.\ i \le n \wedge j \le n \wedge k \le n \longrightarrow M\ i\ k \preceq M\ i\ j \boxplus M\ j\ k$

$$\begin{array}{c|ccc} & \mathbf{0} & c_1 & c_2 \\ \hline \mathbf{0} & \infty & \mathit{Lt}\ (-3) & \mathit{Le}\ 0 \\ c_1 & \infty & \infty & \infty \\ c_2 & \mathit{Le}\ 4 & \infty & \infty \end{array} \longrightarrow \begin{array}{c|ccc} & \mathbf{0} & c_1 & c_2 \\ \hline \mathbf{0} & \mathit{Le}\ 0 & \mathit{Lt}\ (-3) & \mathit{Le}\ 0 \\ c_1 & \infty & \mathit{Le}\ 0 & \infty \\ c_2 & \mathit{Le}\ 4 & \mathit{Lt}\ 1 & \mathit{Le}\ 0 \end{array}$$

  - <u>or</u> negative diagonal entry
  - HOL formulation: recursive function with pointwise updates

# DBM Operations (2)

- Floyd-Warshall algorithm
  - Computes canonical form:
    $\forall\, i\ j\ k.\ i \le n \land j \le n \land k \le n \longrightarrow M\ i\ k \preceq M\ i\ j \boxplus M\ j\ k$

$$\begin{array}{c c} & \begin{array}{ccc} \mathbf{0} & c_1 & c_2 \end{array} \\ \begin{array}{c} \mathbf{0} \\ c_1 \\ c_2 \end{array} & \begin{pmatrix} \infty & Lt\ (-3) & Le\ 0 \\ \infty & \infty & \infty \\ Le\ 4 & \infty & \infty \end{pmatrix} \end{array} \longrightarrow \begin{array}{c c} & \begin{array}{ccc} \mathbf{0} & c_1 & c_2 \end{array} \\ \begin{array}{c} \mathbf{0} \\ c_1 \\ c_2 \end{array} & \begin{pmatrix} Le\ 0 & Lt\ (-3) & Le\ 0 \\ \infty & Le\ 0 & \infty \\ Le\ 4 & Lt\ 1 & Le\ 0 \end{pmatrix} \end{array}$$

  - <u>or</u> negative diagonal entry

# DBM Operations (2)

- Intersection $And\ A\ B \equiv \lambda i\ j.\ min\ (A\ i\ j)\ (B\ i\ j)$
  - $[A]_{v,n} \cap [B]_{v,n} = [And\ A\ B]_{v,n}$
- Reset
  - Want $u\ c = d$ if $u \in [reset\ M\ n\ c\ d]_{v,n}$

  → $(reset\ M\ n\ c\ d)\ c\ 0 = Le\ d$ and $(reset\ M\ n\ c\ d)\ 0\ c = Le\ (-d)$
  - All other constraints regarding *c* invalidated (i.e. set to ∞)
  - Correctness:

$$\{[cs \to d]u \mid u.\, u \in [M]_{v,n}\} = [reset'\ M\ n\ cs\ v\ d]_{v,n}$$

- Similarly delay and intersection with clock constraints

# DBM Semantics

- Symbolic zone semantics

$$\frac{M_i = abstr\ I(l)\ v}{A \vdash \langle l, M \rangle \rightsquigarrow_{v,n} \langle l, up\,(M \sqcap M_i) \sqcap M_i \rangle}$$

$$\frac{A \vdash l \longrightarrow^{g,a,r} l' \qquad M_i = abstr\ I(l')\ v}{A \vdash \langle l, M \rangle \rightsquigarrow_{v,n} \langle l', reset'\ (M \sqcap abstr\ g\ v)\ n\ r\ v\ 0 \sqcap M_i \rangle}$$

- Compare
- Sound & complete w.r.t. zone semantics
- Symbolic computation procedure for reachability but infinite search space

# DBM Semantics

- Symbolic zone semantics

$$\frac{M_i = abstr\ I(l)\ v}{A \vdash \langle l, M\rangle \rightsquigarrow_{DBM} \langle l, up\,(M \sqcap M_i) \sqcap M_i\rangle}$$

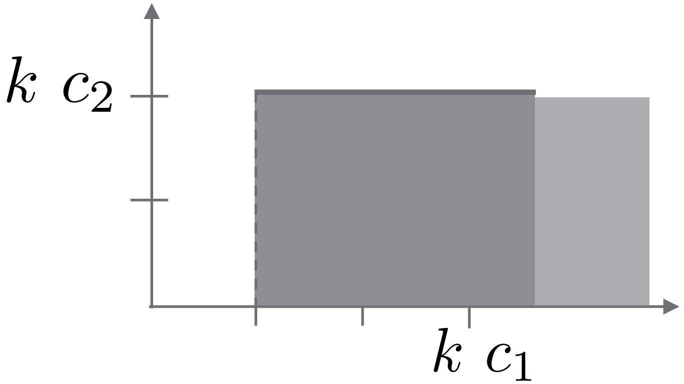
$$\frac{A \vdash l \longrightarrow^{g,a,r} l' \qquad M_i = abstr\ I(l')\ v}{A \vdash \langle l, M\rangle \rightsquigarrow_{DBM} \langle l', reset'\,(M \sqcap abstr\ g\ v)\ n\ r\ v\ 0 \sqcap M_i\rangle}$$

- Sound & complete w.r.t. zone semantics
- Symbolic computation procedure for reachability but infinite search space

# Obtaining a Finite Search Space

- Goal: Only compute finitely many different matrices
  - Idea: cut off DBM entries at maximal constant of automaton for each clock

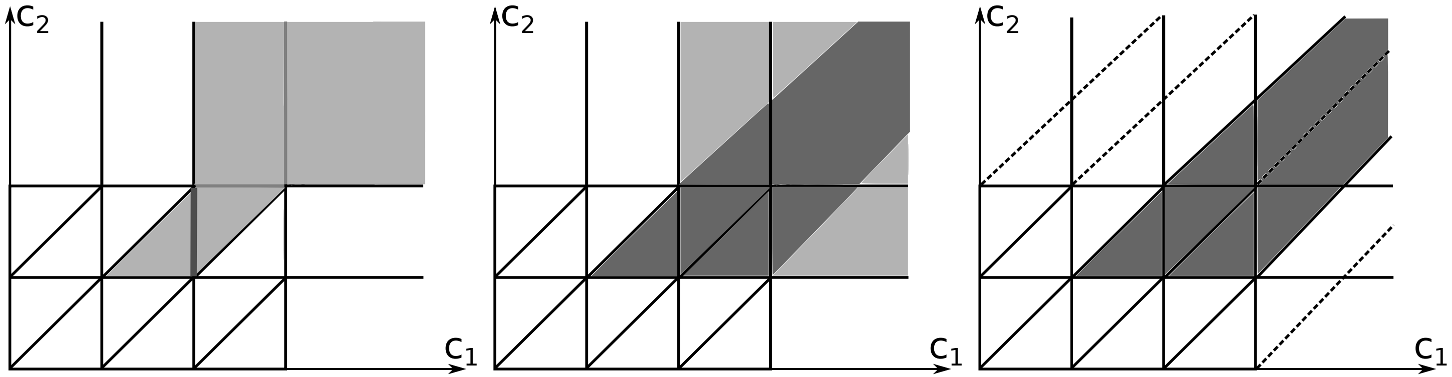
→ Normalization
  - Clock ceiling $k :: {}'c \Rightarrow nat$




  - Proving that this preserves reachability is the hardest part

# Regions

- Regions: partition of zones that yields a correct abstraction



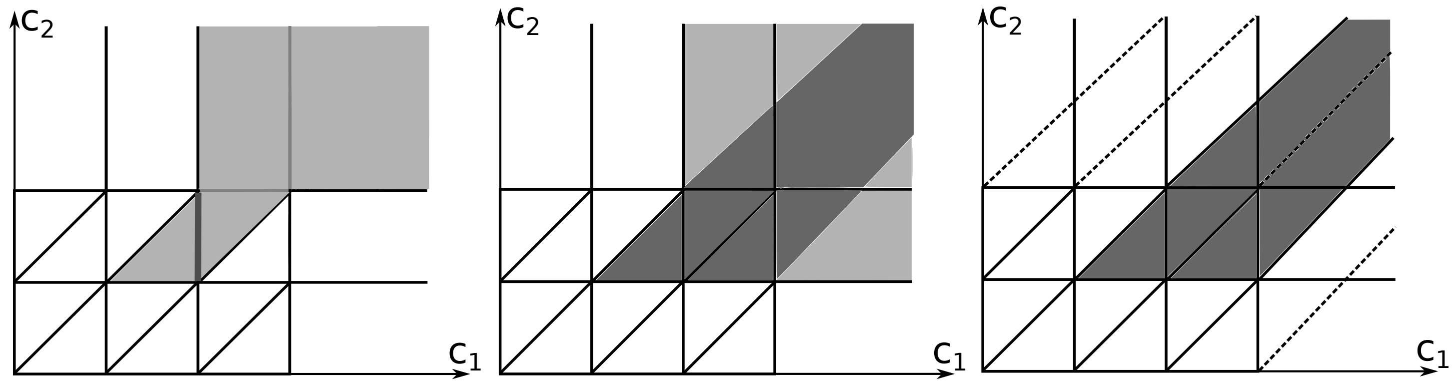

- Approximating zones with regions (not convex):

$$Closure_\alpha\ Z = \bigcup \{R \in \mathcal{R} \mid R \cap Z \neq \emptyset\}$$

- Convex approximation:

# Regions

- Regions: partition of zones that yields a correct abstraction




- Approximating zones with regions (not convex):

$$Closure_\alpha\ Z = \bigcup\{R \in \mathcal{R} \mid R \cap Z \neq \emptyset\}$$

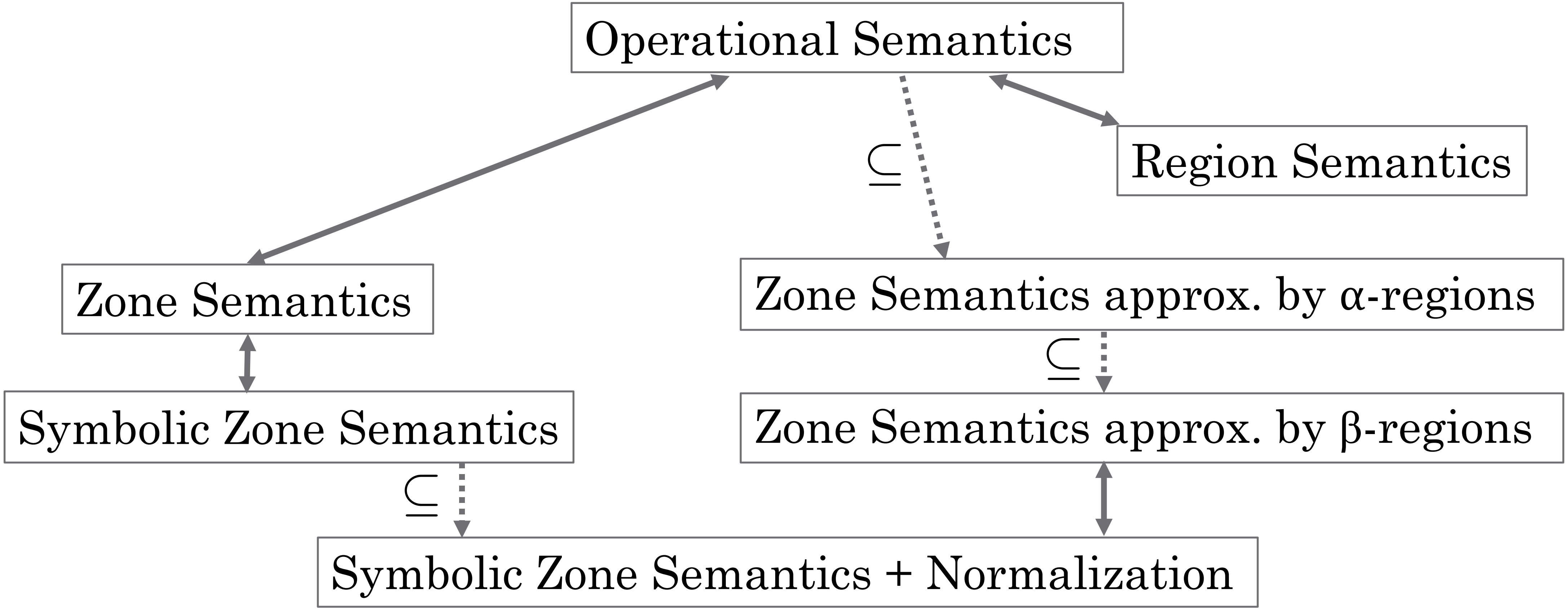
- Convex approximation: $Approx_\beta\ Z$

# Semantics Zoo

$$
\begin{tikzcd}
 & \boxed{A \vdash \langle l, u\rangle \rightarrow \langle l', u'\rangle} \arrow[r, leftrightarrow] \arrow[dl, leftrightarrow] \arrow[dr, dotted, "\subseteq"'] & \boxed{A, \mathcal{R}_\alpha \vdash \langle l, R\rangle \rightsquigarrow \langle l', R'\rangle} \\
\boxed{A \vdash \langle l, Z\rangle \rightsquigarrow \langle l', Z'\rangle} \arrow[d, leftrightarrow] & & \boxed{A \vdash \langle l, Z\rangle \rightsquigarrow_\alpha \langle l', Closure_\alpha\, Z'\rangle} \arrow[d, dotted, "\subseteq"'] \\
\boxed{A \vdash \langle l, M\rangle \rightsquigarrow_{v,n} \langle l', M'\rangle} \arrow[dr, dotted, "\subseteq"'] & & \boxed{A \vdash \langle l, Z\rangle \rightsquigarrow_\beta \langle l', Approx_\beta\, Z'\rangle} \arrow[dl, leftrightarrow] \\
 & \boxed{A \vdash \langle l, M\rangle \rightsquigarrow_{\mathcal{N}} \langle l', norm\,(FW\ M'\ n)\ k\ n\rangle} &
\end{tikzcd}
$$

$$
\begin{aligned}
&(\exists u \in [M]_{v,n}.\ \exists u'.\ A \vdash \langle l, u\rangle \rightarrow^* \langle l', u'\rangle) \\
\longleftrightarrow\ &(\exists M'.\ A \vdash \langle l, M\rangle \rightsquigarrow_{\mathcal{N}}{}^* \langle l', M'\rangle \wedge [M']_{v,n} \neq \emptyset)
\end{aligned}
$$

# Semantics Zoo




Given start state $(l, u)$ and destination $l'$, is there a run $A \vdash (l, u) \to^* (l', u')$ for some $u'$?

# Conclusion

- Current Formalization
  - All important notions for timed automata: regions, zones, DBMs
  - Correctness of symbolic reachability analysis using DBMs
  - ~ 16.000 lines of code, available in the AFP
- Future / ongoing work
  - Executable reachability analysis with imperative algorithms
  - Fully verified model checking → needs modelling features such as networks of timed automata
  - Decidability of reachability for probabilistic TA via region construction

# Related Work

- Forward reachability via region construction in PVS
  - Qingguo Xu and Huaikou Miao
  - Establishes decidability, no symbolic analysis
- Framework for p-automata in Coq
  - Christine Paulin-Mohring
  - Scope: reasoning about (priced) timed automata in Coq
  - No meta-theory on model checking
- Timed Automata Modeling Environment in PVS
  - Myla Archer and Constance Heitmeyer
  - Similarly: no meta-theory on model checking