Real-time and Probabilistic Systems Verification

Luca Tesei

MSc in Computer Science, University of Camerino

Topics

- Reachability with zones.

More:

The slides in the following pages are taken from the material of the course “Advanced Model Checking” held by Prof. Dr. Ir. Joost-Pieter Katoen at Aachen University.

TCTL model checking

- Model checking timed automata against TCTL is decidable
  - example TCTL-formula: $\forall\Diamond^{\leqslant 10}$*goal*
- Key ingredient for decidability: finite quotient wrt. a bisimulation
  - bisimulation = equivalence on clock valuations
  - equivalence classes are called *regions*
- Region automaton is highly impractical for tool implementation
  - the number of regions lies in $\Theta(|C|! \cdot \prod_{x \in C} c_x)$
- In practice, coarser abstractions than regions are used
  - this lecture considers time-bounded reachability using *zones*

Reachability analysis

- Forward analysis:
  - starting from some initial configuration
  - determine configurations that are reachable within 1, 2, 3, . . . steps
  - until either the goal configuration is reached, or the computation terminates
- Backward analysis:
  - starting from the goal configuration
  - determine configurations that can reach the goal within 1, 2, 3, . . . steps
  - until either the initial configuration is reached, or the computation terminates

how can these approaches be realized for timed automata?

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 $e = \ell \xhookrightarrow{g:\alpha,D} \ell'$ let:

$$Post_e(z) = \{ \eta' \in \mathbb{R}^n_{\geqslant 0} \mid \exists \eta \in z,\ d \in \mathbb{R}_{\geqslant 0}.\ \eta{+}d \models g \wedge \eta' = \text{reset } D \text{ in } (\eta{+}d) \}$$

$$Pre_e(z) = \{ \eta \in \mathbb{R}^n_{\geqslant 0} \mid \exists \eta' \in z,\ d \in \mathbb{R}_{\geqslant 0}.\ \eta{+}d \models g \wedge \eta' = \text{reset } D \text{ in } (\eta{+}d) \}$$

- Intuition:
  - $\eta' \in Post_e(z)$ if for some $\eta \in z$ and delay d, $(\ell, \eta) \xrightarrow{d} \ldots \xrightarrow{e} (\ell', \eta')$
  - $\eta \in Pre_e(z)$ if for some $\eta' \in z$ and delay d, $(\ell, \eta) \xrightarrow{d} \ldots \xrightarrow{e} (\ell', \eta')$

Zones

- Clock constraints are *conjunctions* of constraints of the form:
  - $x \prec c$ and $x - y \prec c$ for $\prec \in \{ <, \leqslant, =, \geqslant, > \}$, and $c \in \mathbb{Z}$
- A *zone* is a set of clock valuations satisfying a clock constraint
  - a clock zone for g is the set of clock valuations satisfying g
- Clock zone of g: $[\![g]\!] = \{ \eta \in \mathit{Eval}(C) \mid \eta \models g \}$
- The *state zone* of $s = \langle \ell, \eta \rangle$ is $\langle \ell, z \rangle$ with $\eta \in z$
- For *zone* z and edge e, $\mathit{Post}_e(z)$ and $\mathit{Pre}_e(z)$ are *zones*

state zones will be used as symbolic representations for configurations

Operations on zones

- Future of z:
  - $\overrightarrow{z} = \{ \eta + d \mid \eta \in z \wedge d \in \mathbb{R}_{\geqslant 0} \}$
- Past of z:
  - $\overleftarrow{z} = \{ \eta - d \mid \eta \in z \wedge d \in \mathbb{R}_{\geqslant 0} \}$
- Intersection of two zones:
  - $z \cap z' = \{ \eta \mid \eta \in z \wedge \eta \in z' \}$
- Clock reset in a zone:
  - reset D in $z = \{$ reset D in $\eta \mid \eta \in z \}$
- Inverse clock reset of a zone:
  - reset^{-1} D in $z = \{ \eta \mid$ reset D in $\eta \in z \}$

Symbolic successors and predecessors

Recall that for edge $e = \ell \xrightarrow{g:\alpha,D} \ell'$ we have:

$$\mathit{Post}_e(z) \;=\; \{\, \eta' \in \mathbb{R}^n_{\geqslant 0} \mid \exists \eta \in z,\; d \in \mathbb{R}_{\geqslant 0}.\; \eta{+}d \models g \wedge \eta' = \text{reset } D \text{ in } (\eta{+}d) \,\}$$

$$\mathit{Pre}_e(z) \;=\; \{\, \eta \in \mathbb{R}^n_{\geqslant 0} \mid \exists \eta' \in z,\; d \in \mathbb{R}_{\geqslant 0}.\; \eta{+}d \models g \wedge \eta' = \text{reset } D \text{ in } (\eta{+}d) \,\}$$

This can also be expressed symbolically using operations on zones:

$$\mathit{Post}_e(z) \;=\; \text{reset } D \text{ in } (\overrightarrow{z} \cap [\![\, g \,]\!])$$

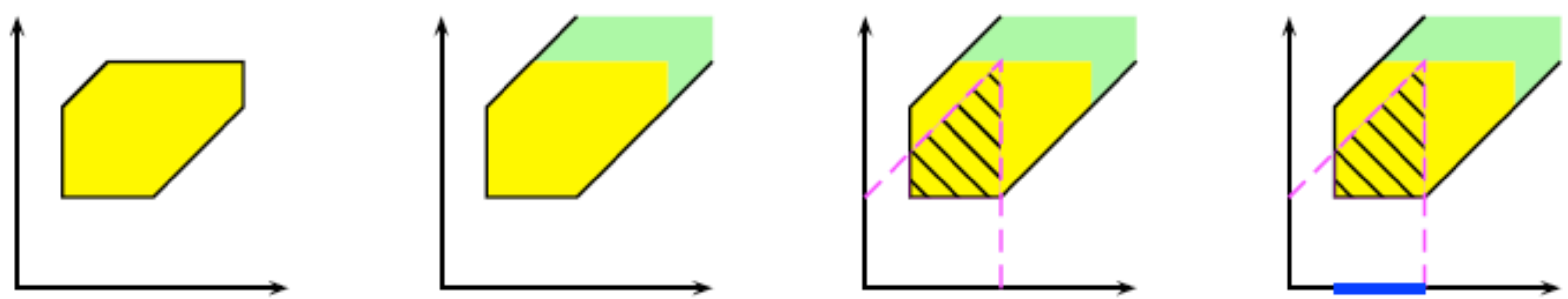
and

$$\mathit{Pre}_e(z) \;=\; \overleftarrow{\text{reset}^{-1}\; D \text{ in } (z \cap [\![\, D = 0 \,]\!]) \cap [\![\, g \,]\!]}$$

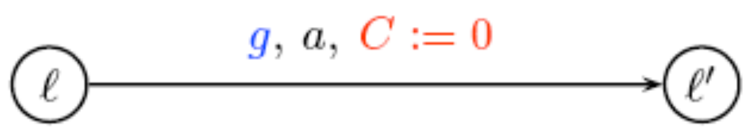
Zone successor: example

$$\ell \xrightarrow{g,\ a,\ C := 0} \ell'$$

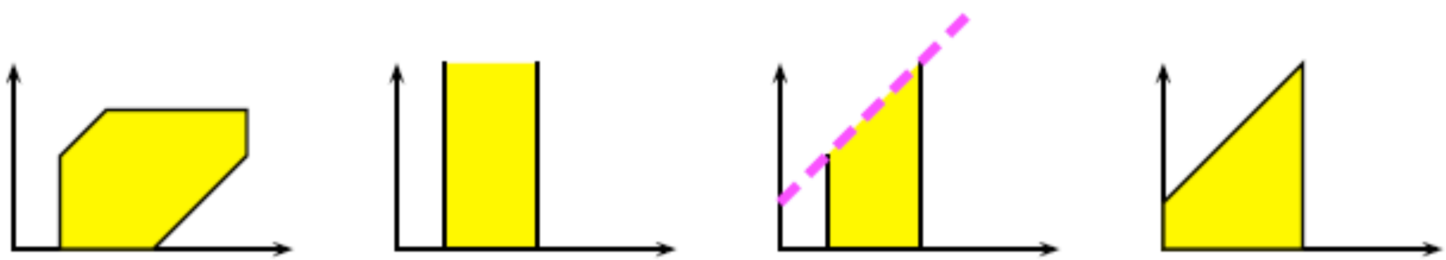
zones	Z	$[C \leftarrow 0](\overrightarrow{Z} \cap g)$



Zone predecessor: example



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



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

Backward symbolic transition system (1)

Backward symbolic transition system of *TA* with $|C| = n$ is inductively defined by:

$$\frac{e = \ell \xleftarrow{g:\alpha,D}\!\!\!\rightarrow \ell' \qquad z = \mathit{Pre}_e(z')}{(\ell', z') \Leftarrow (\ell, z)}$$

Iterative backward reachability analysis computation schemata:

$$\begin{array}{rcl} T_0 & = & \{\, (\ell, \mathbb{R}^n_{\geqslant 0}) \mid \ell \text{ is a goal location} \,\} \\ T_1 & = & T_0 \cup \{\, (\ell, z) \mid \exists (\ell', z') \in T_0 \text{ such that } (\ell', z') \Leftarrow (\ell, z) \,\} \\ \ldots & & \ldots \\ T_{k+1} & = & T_k \cup \{\, (\ell, z) \mid \exists (\ell', z') \in T_k \text{ such that } (\ell', z') \Leftarrow (\ell, z) \,\} \\ \ldots & & \ldots \end{array}$$

until either the computation stabilizes or reaches an initial configuration (ℓ_0, z_0)

Backward symbolic transition system (2)

Backward symbolic transition system of *TA* is inductively defined by:

$$\frac{e = \ell \xhookleftarrow{g:\alpha,D} \ell' \qquad z = \mathit{Pre}_e(z')}{(\ell', z') \Leftarrow (\ell, z)}$$

Iterative backward reachability analysis computation schemata:

$$\begin{array}{rcl}
T_0 & = & \{ (\ell, \mathbb{R}^n_{\geqslant 0}) \mid \ell \text{ is a goal location} \} \\
T_1 & = & T_0 \cup \{ (\ell, z) \mid \exists (\ell', z') \in T_0.\, (\ell', z') \Leftarrow (\ell, z) \text{ and } \ell' = \ell \text{ implies } z \not\subseteq z' \} \\
\ldots & & \ldots \\
T_{k+1} & = & T_k \cup \{ (\ell, z) \mid \exists (\ell', z') \in T_k.\, (\ell', z') \Leftarrow (\ell, z) \text{ and } \ell' = \ell \text{ implies } z \not\subseteq z' \} \\
\ldots & & \ldots
\end{array}$$

until either the computation stabilizes or reaches an initial configuration (ℓ_0, z_0)

Termination and correctness [Henzinger et al., 1994]

The backward computation terminates and is correct wrt. reachability properties

Because of the bisimulation property, it holds:

Every set of valuations which is computed along the backward computation is a finite union of regions

Forward reachability analysis (1)

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

$$\frac{e = \ell \xhookrightarrow{g:\alpha,D} \ell' \qquad z' = \mathit{Post}_e(z)}{(\ell, z) \Rightarrow (\ell', z')}$$

Iterative forward reachability analysis computation schemata:

$$\begin{array}{rcl} T_0 & = & \{ (\ell_0, z_0) \mid \forall x \in C.\, z_0(x) = 0 \} \\ T_1 & = & T_0 \cup \{ (\ell', z') \mid \exists (\ell, z) \in T_0 \text{ such that } (\ell, z) \Rightarrow (\ell', z') \} \\ \ldots & & \ldots \\ T_{k+1} & = & T_k \cup \{ (\ell', z') \mid \exists (\ell, z) \in T_k \text{ such that } (\ell, z) \Rightarrow (\ell', z') \} \\ \ldots & & \ldots \end{array}$$

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:

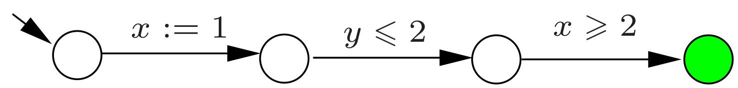
$$\frac{e = \ell \xrightarrow{g:\alpha,D} \ell' \qquad z' = \mathit{Post}_e(z)}{(\ell, z) \Rightarrow (\ell', z')}$$

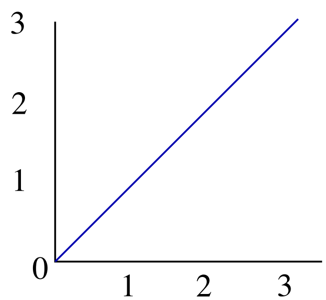
Iterative forward reachability analysis computation schemata:

$$\begin{array}{rcl}
T_0 & = & \{\, (\ell_0, z_0) \mid \forall x \in C.\ z_0(x) = 0 \,\} \\
T_1 & = & T_0 \cup \{\, (\ell', z') \mid \exists (\ell, z) \in T_0.\ (\ell, z) \Rightarrow (\ell', z') \text{ and } \ell = \ell' \text{ implies } z \not\subseteq z' \,\} \\
\ldots & & \ldots \\
T_{k+1} & = & T_k \cup \{\, (\ell', z') \mid \exists (\ell, z) \in T_k.\ (\ell, z) \Rightarrow (\ell', z') \text{ and } \ell = \ell' \text{ implies } z \not\subseteq z' \,\} \\
\ldots & & \ldots
\end{array}$$

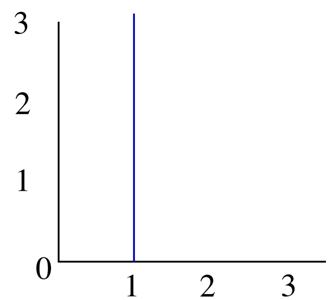
until either the computation stabilizes or reaches a symbolic state containing a goal configuration

Forward reachability analysis: intuition

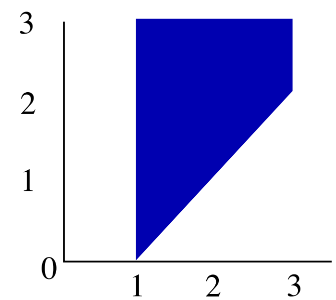




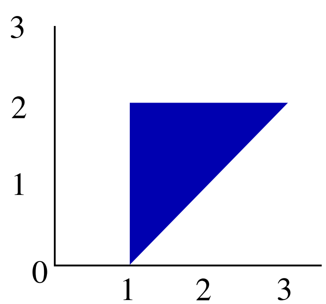
leaving initial



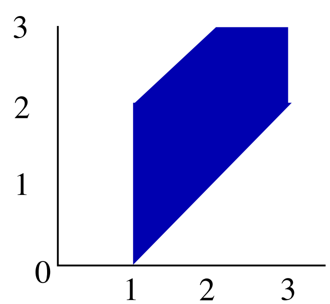
entering first



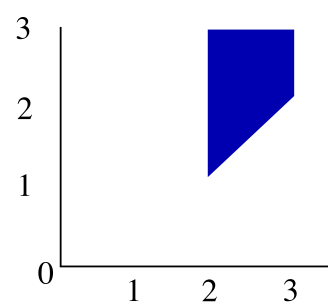
leaving first



entering second



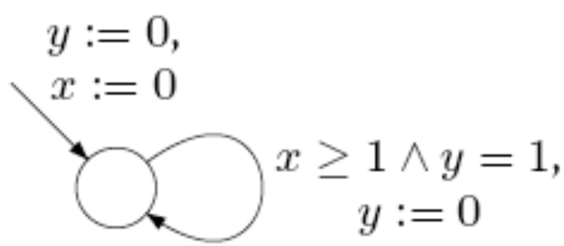
leaving second

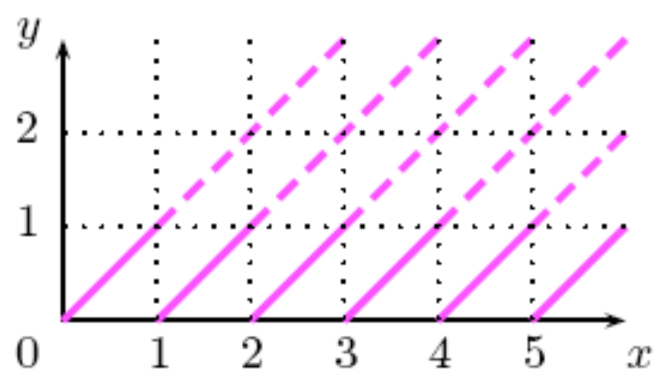


entering third

Possible non-termination

The forward analysis is correct but may not terminate:





➡ an infinite number of steps...

Solution: abstract forward reachability

Let γ associate sets of valuations to sets of valuations

Abstract forward symbolic transition system of *TA* is defined by:

$$\frac{(\ell, z) \Rightarrow (\ell', z') \qquad z = \gamma(z)}{(\ell, z) \Rightarrow_{\gamma} (\ell', \gamma(z'))}$$

Iterative forward reachability analysis computation schemata:

$$\begin{array}{rcl} T_0 & = & \{ (\ell_0, \gamma(z_0)) \mid \forall x \in C.\, z_0(x) = 0 \} \\ T_1 & = & T_0 \cup \{ (\ell', z') \mid \exists (\ell, z) \in T_0 \text{ such that } (\ell, z) \Rightarrow_{\gamma} (\ell', z') \} \\ \ldots & & \ldots \\ T_{k+1} & = & T_k \cup \{ (\ell', z') \mid \exists (\ell, z) \in T_k \text{ such that } (\ell, z) \Rightarrow_{\gamma} (\ell', z') \} \\ \ldots & & \ldots \end{array}$$

with inclusion check and termination criteria as before

Soundness and correctness

- Soundness:

$$\underbrace{\langle \ell_0, \gamma(z_0) \rangle \Rightarrow_{\gamma}^{*} \langle \ell, z \rangle}_{\text{abstract symbolic reachability}} \quad \text{implies} \quad \exists\, \underbrace{\langle \ell_0, \eta_0 \rangle \rightarrow^{*} \langle \ell, \eta \rangle}_{\text{reachability in } \mathit{TS}(\mathit{TA})} \text{ with } \eta \in z$$

- Completeness:

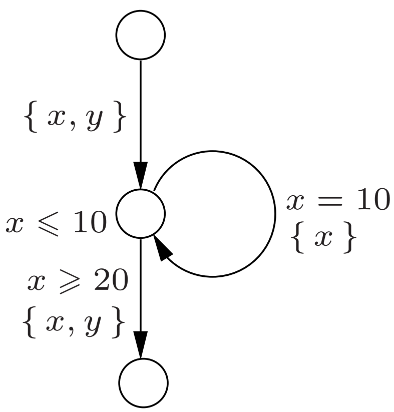
$$\underbrace{\langle \ell_0, \eta_0 \rangle \rightarrow^{*} \langle \ell, \eta \rangle}_{\text{reachability in } \mathit{TS}(\mathit{TA})} \quad \text{implies} \quad \exists\, \underbrace{\langle \ell_0, \gamma(\{\, \eta_0 \,\}) \rangle \Rightarrow_{\gamma}^{*} \langle \ell, z \rangle}_{\text{abstract symbolic reachability}} \text{ for some } z \text{ with } \eta \in z$$

for any choice of γ, soundness and completeness are desirable

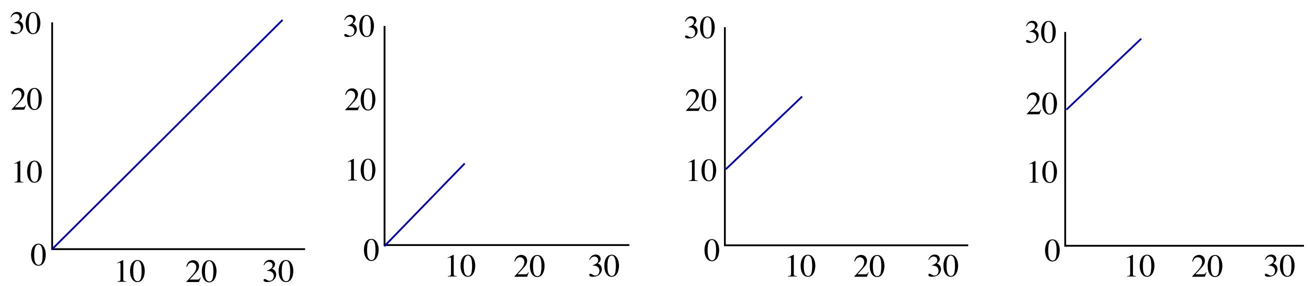
Criteria on the abstraction operator

- Finiteness: $\{\, \gamma(z) \mid \gamma$ defined on $z \,\}$ is finite
- Correctness: γ is sound wrt. reachability
- Completeness: γ is complete wrt. reachability
- Effectiveness: γ is defined on zones, and $\gamma(z)$ is a zone

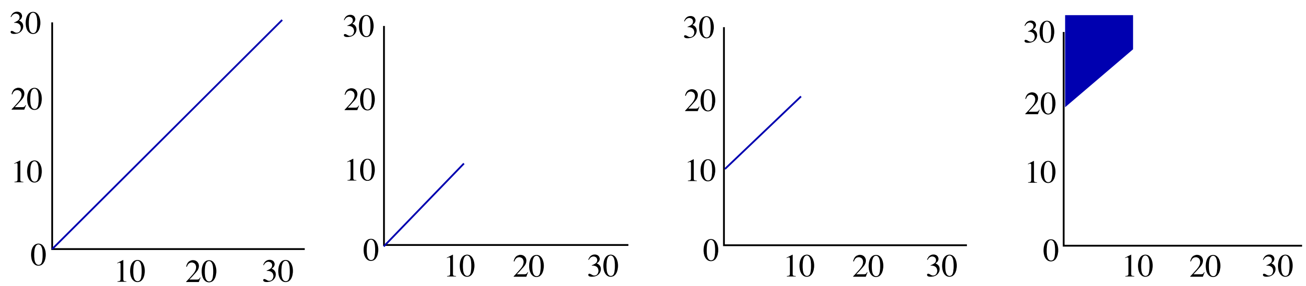
Normalization: intuition



symbolic semantics has infinitely many zones:



normalization yields a finite zone graph:

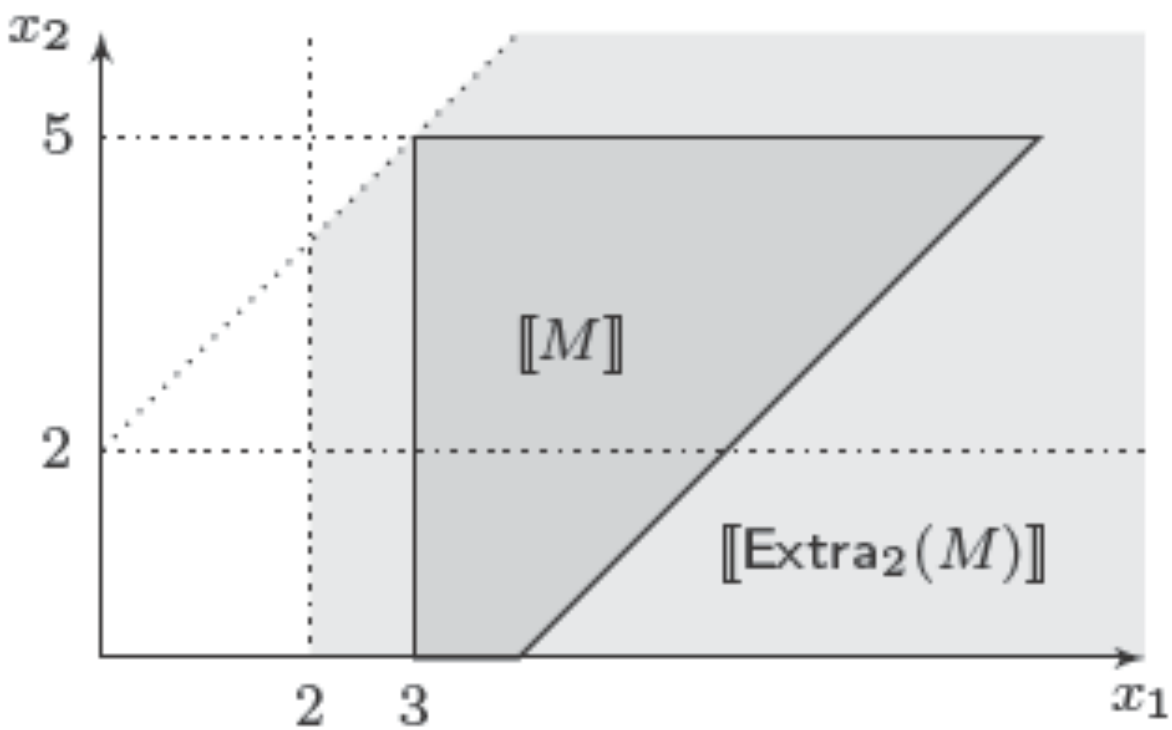


k-Normalization [Daws & Yovine, 1998]

Let $k \in \mathbb{N}$.

- A k-bounded zone is described by a k-bounded clock constraint
  - e.g., zone $z = (x \geqslant 3) \wedge (y \leqslant 5) \wedge (x - y \leqslant 4)$ is not 2-bounded
  - but zone $z' = (x \geqslant 2) \wedge (y - x \leqslant 2)$ is 2-bounded
  - note that: $z \subseteq z'$
- Let *norm*$_k(z)$ be the smallest k-bounded zone containing zone z

Example of k-normalization



Facts about k-normalization [Bouyer, 2003]

- Finiteness: *norm*$_k(\cdot)$ is a finite abstraction operator
- Correctness: *norm*$_k(\cdot)$ is sound wrt. reachability

  provided k is the maximal constant appearing in the constraints of *TA*
- Completeness: *norm*$_k(\cdot)$ is complete wrt. reachability

  since $z \subseteq$ *norm*$_k(z)$, so *norm*$_k(\cdot)$ is an over-approximation
- Effectiveness: *norm*$_k(z)$ is a zone

  this will be made clear in the sequel when considering zone representations