Difference Bound Matrices

Lecture #18 of Advanced Model Checking

Joost-Pieter Katoen

Lehrstuhl 2: Software Modeling & Verification

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

July 8, 2009

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:

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

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

- Intuition:
  - $\eta' \in Post_e(z)$ if for some $\eta \in z$ and delay d, $(\ell, \eta) \xRightarrow{d} \ldots \xrightarrow{e} (\ell', \eta')$
  - $\eta \in \textit{Pre}_e(z)$ 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 maximal 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 $e = \ell \xhookrightarrow{g:\alpha,D} \ell'$ we have:

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

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

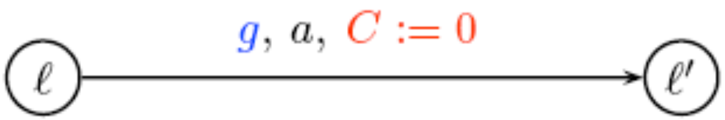
This can also be expressed symbolically using operations on zones:

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

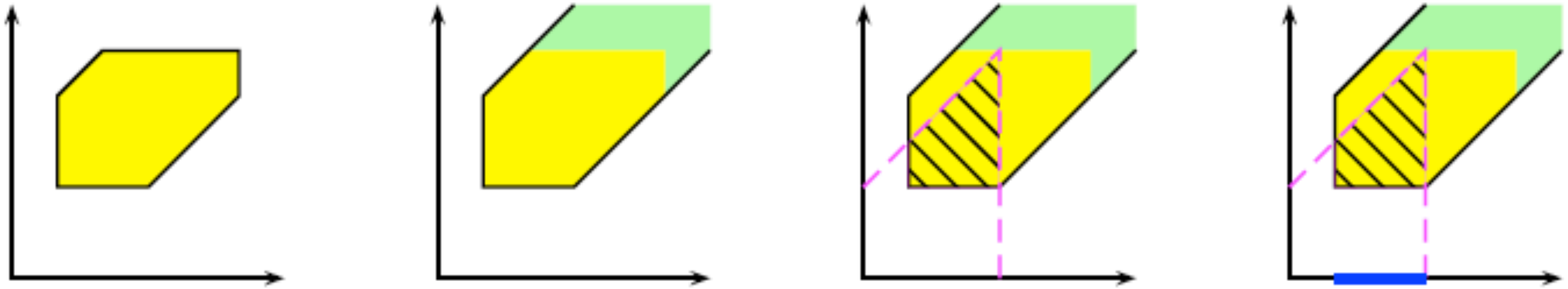
and

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

Zone successor: example

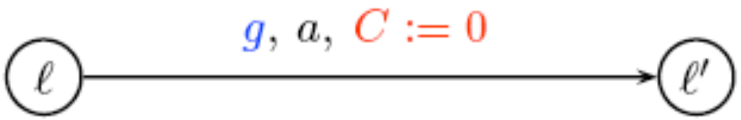


zones Z $[C \leftarrow 0](\overrightarrow{Z} \cap g)$

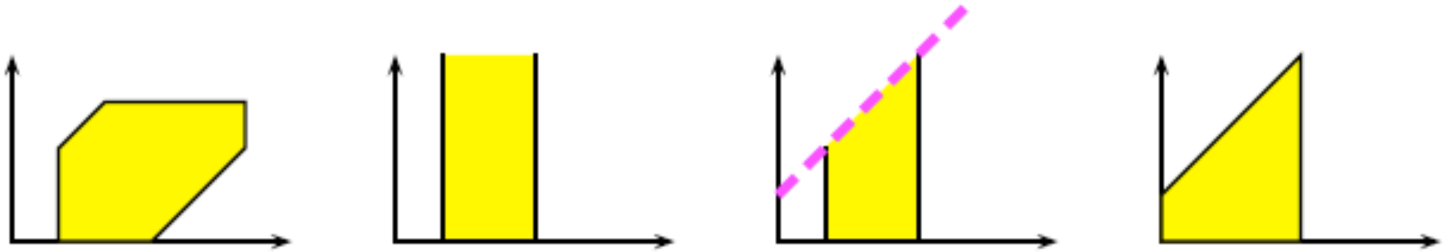


Z $\overrightarrow{Z}$ $\overrightarrow{Z} \cap g$ $[y \leftarrow 0](\overrightarrow{Z} \cap g)$

Zone predecessor: example



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



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

Forward reachability analysis (1)

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

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

Iterative forward reachability analysis computation schemata:

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

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:

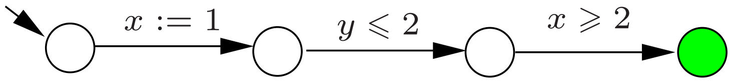
$$\frac{e = \left(\ell \xrightarrow{g:\alpha,D} \ell'\right) \qquad z' = \mathit{Post}_e(z)}{(\ell, z) \Rightarrow (\ell', z')}$$

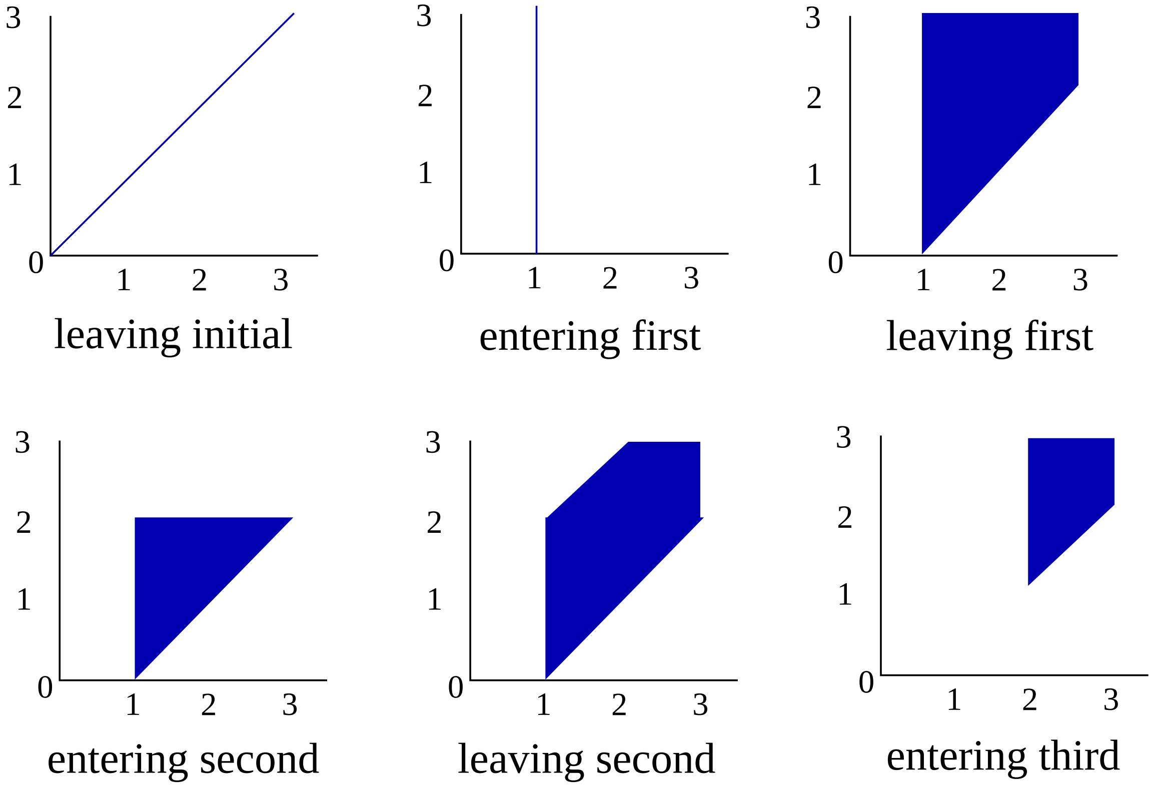
Iterative forward reachability analysis computation schemata:

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

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

Forward reachability analysis: intuition





leaving initial

entering first

leaving first

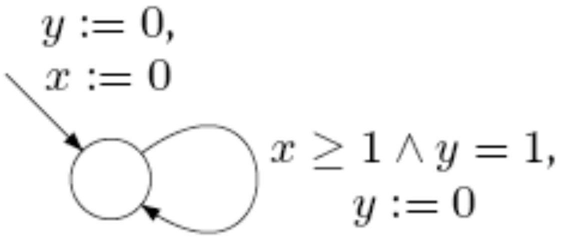
entering second

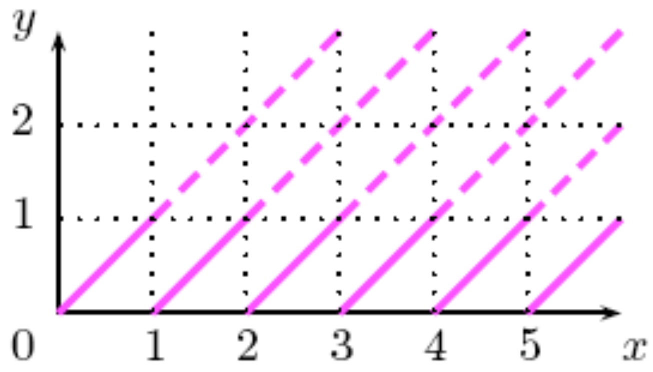
leaving second

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:

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

- Completeness:

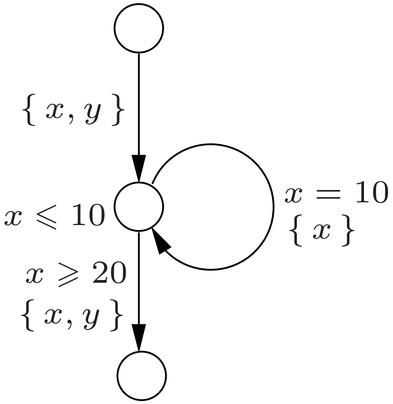
$$\underbrace{\langle \ell_0, \eta_0 \rangle \longrightarrow^{*} \langle \ell, \eta \rangle}_{\text{reachability in } TS(TA)} \quad \text{implies} \quad \exists\, \underbrace{\langle \ell_0, \gamma(\{\, \eta_0 \,\}) \rangle \Rightarrow_{\gamma}^{*} \langle \ell, z \rangle}_{\text{abstract symbolic reachability}}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

for any choice of γ, soundness and completeness are desirable

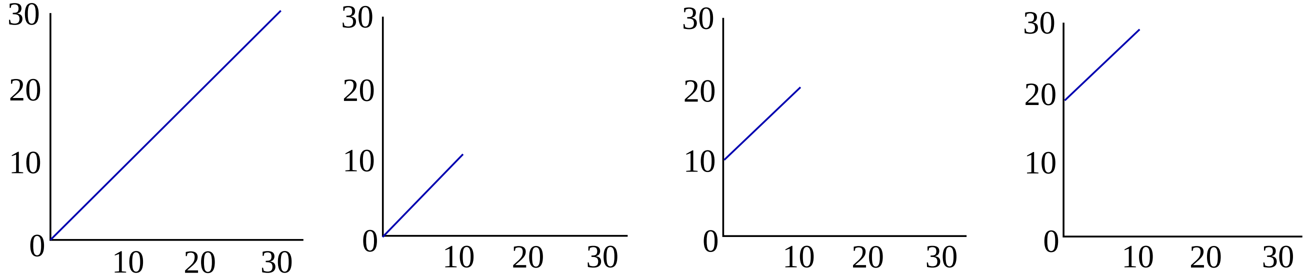
Criteria on the abstraction operator

- 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

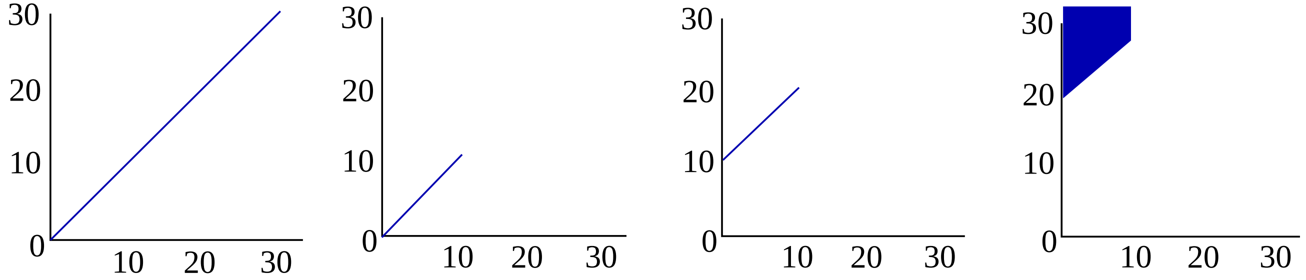
Normalization: intuition



symbolic semantics has infinitely many zones:



normalization yields a finite zone graph:

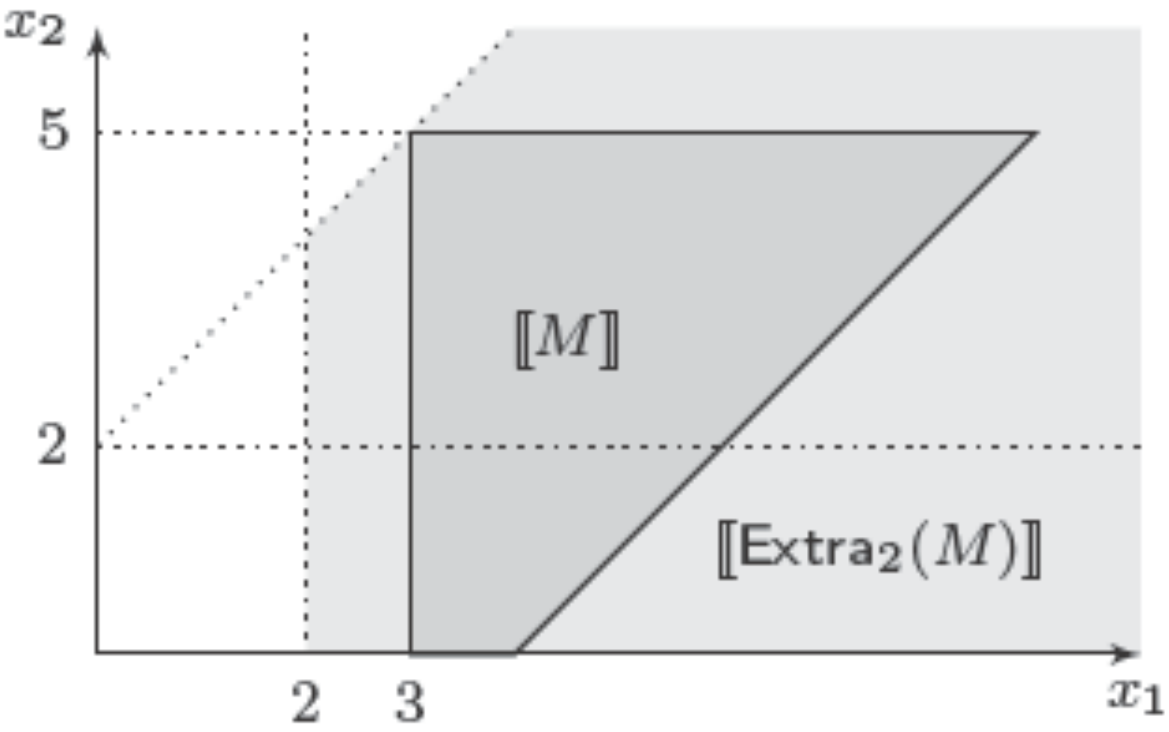


k-Normalization [Daws & Yovine, 1998]

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

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:

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

- 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., $\mathbf{0} - x_i \leqslant 0$ all clocks are positive
  - $\mathbf{Z}(i,i) := (0, \leqslant)$, i.e., each clock equals itself

Example

$$(x_1 \geq 3) \wedge (x_2 \leq 5) \wedge (x_1 - x_2 \leq 4) \qquad \begin{array}{cc} & \begin{array}{ccc} x_0 & x_1 & x_2 \end{array} \\ \begin{array}{c} x_0 \\ x_1 \\ x_2 \end{array} & \begin{pmatrix} +\infty & -3 & +\infty \\ +\infty & +\infty & 4 \\ 5 & +\infty & +\infty \end{pmatrix} \end{array}$$

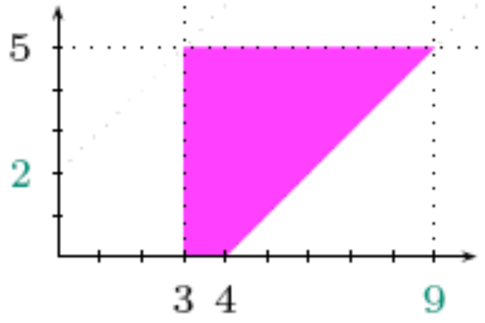
all clock constraints in the above DBM are of the form $(c, \leqslant)$

The need for canonicity

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

$$\begin{array}{c} \\ x_0 \\ x_1 \\ x_2 \end{array} \begin{array}{c} \begin{array}{ccc} x_0 & x_1 & x_2 \end{array} \\ \left(\begin{array}{ccc} +\infty & \mathbf{-3} & +\infty \\ +\infty & +\infty & \mathbf{4} \\ \mathbf{5} & +\infty & +\infty \end{array} \right) \end{array}$$

- Existence of a normal form



$$\begin{pmatrix} 0 & \mathbf{-3} & 0 \\ 9 & 0 & \mathbf{4} \\ \mathbf{5} & 2 & 0 \end{pmatrix}$$

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 $c < c'$
- Addition of DBM entries:
  - $c + \infty = \infty$
  - $(c, \leqslant) + (c', \leqslant) = (c{+}c', \leqslant)$
  - $(c, <) + (c', \leqslant) = (c{+}c', <)$

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 $[\![\, \mathbf{Z} \wedge g \,]\!] = \varnothing$

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 $(0, \preceq)$

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

  - $\mathbf{Z}$ 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 $\mathbf{Z}(j,i) := \mathbf{Z}(j,0) + (-d, \leqslant)$

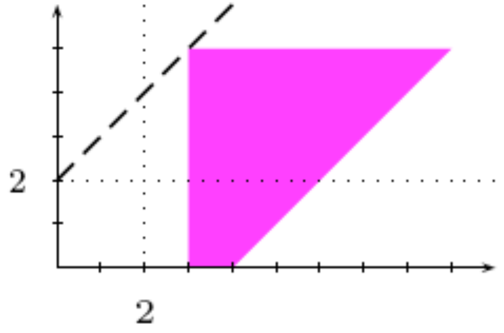
- *k-Normalization*: *norm*$_k(\mathbf{Z})$
  - remove all bounds $x - y \preceq m$ for which $(m, \preceq) > (k, \leqslant)$, and
  - set all bounds $x - y \preceq m$ with $(m, \preceq) < (-k, <)$ to $(-k, <)$
  - put the DBM back into canonical form (Floyd-Warshall)

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 $-k$