Recall: Number of Regions

Lemma 4.28. Let $X$ be a set of clocks, $c_x \in \mathbb{N}_0$ the maximal constant for each $x \in X$, and $c = \max\{c_x | x \in X\}$. Then $(2c + 2)|X| \cdot (4c + 3)^{1/2}|X| \cdot (|X| - 1)$ is an upper bound on the number of regions.

In the desk lamp controller,

\[
\begin{align*}
\langle \text{off}, \{0\} \rangle &\xrightarrow{\text{press} \ ?} \langle \text{light}, \{0\} \rangle, \\
\langle \text{light}, \{0\} \rangle &\xrightarrow{\text{press} \ ?} \langle \text{bright}, \{(0, 1)\} \rangle, \\
&\quad \ldots, \\
\langle \text{light}, \{0\} \rangle &\xrightarrow{\text{press} \ ?} \langle \text{bright}, \{(2, 3)\} \rangle, \\
\langle \text{light}, \{0\} \rangle &\xrightarrow{\text{press} \ ?} \langle \text{bright}, \{3\} \rangle.
\end{align*}
\]

Which seems to be a complicated way to write just:

\[
\langle \text{light}, \{0\} \rangle \xrightarrow{\text{press} \ ?} \langle \text{bright}, \{0, 3\} \rangle.
\]

Can't we constructively abstract $L$ to:

\[
\langle \text{off}, \{0\} \rangle \langle \text{light}, \{0\} \rangle \langle \text{bright}, \{0, 3\} \rangle \langle \text{off}, \{3, \infty\} \rangle \langle \text{off}, \{0, \infty\} \rangle.
\]
Zones-based Reachability Analysis

Definition. A (closed) clock zone is a set $Z$ of valuations of clocks such that $Z = \{ \nu \mid \varphi(\nu) \}$ where $\varphi$ is a clock constraint.

Example. What is a Zone?

$x > 0 \wedge 2 < y \wedge y > 0 \wedge x < 3$

$x > 0 \wedge y < 2 \wedge (x > 3) \vee (y < 1) \vee (x \leq 5) = \emptyset$

A zone is a closed subset of $\mathbb{R}^n$.

More Examples: Zone or Not?

Zone or Not Zone

Regions

Discussion

(reduction criterion).

Motivation

Zone-based Reachability Analysis

• Given a system $\ell$, a procedure to compute $e_\ell$ yields the configuration $\langle z_\ell, e_\ell \rangle$.

• $z_\ell$, $e_\ell$ corresponds to $z_{\ell, \alpha}$ in DBMs.

• Not all reachable configurations from a configuration $x$ are in $z_{\ell, \alpha}$.

• $e_\ell$ is a symbolic $\bullet$ operator.

• $z_{\ell, \alpha}$ is a zone.

• $z_{\ell, \alpha}$ is a zone if and only if $\Phi(\varphi)$.

Note: Each clock constraint $\varphi$ of valuations of clocks $X$ is a zone by $\Phi(\varphi)$.

But: There is no one-to-one correspondence between clock constraints and zones.
This is Good News...
of \( \phi \) reset clocks

\( \ell \) intersect with invariant

intersect with guard

\( \ell \) (\( \phi \))

\( \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \lland \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)

\( \phi \land \leq y \leq \phi \)
• **Motivation**: Sometimes, regions seem too fine-grained.

• **Definition**

• **Examples**: Zone or Not Zone

• **Zone-based Reachability Analysis**

• **The basic algorithm**

• **Building blocks**:
  - Post-operator,
  - Subsumption check

• **A symbolic Post-operator**

• **Difference-Bounds-Matrices (DBMs)**

• **Discussion**: Zones vs. Regions

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---
A zone is a set of clock valuations which can be characterised by a clock constraint.

Each zone is a union of regions, not every union of regions is a zone.

There is an effectively computable Post-operation for TA edges on zones.

Based on: time elapse, intersection, reset

So there is a fully symbolic decision procedure for location reachability (if we ensure termination by widening)

Even more convenient: using DBMs

Since DBMs have a normal form

For a given model, sometimes the region-based / sometimes the zone-based approach is faster.

Not so many region-based tools are "on the market" these days.

References
