Stutter Bisimulation Quotienting

Lecture #8 of Advanced Model Checking

Joost-Pieter Katoen

Lehrstuhl 2: Software Modeling & Verification

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

November 20, 2006

Motivation

- Quotienting wrt. $\approx^{div}$ allows to *abstract from stutter steps*
  - in particular $TS \approx^{div} TS/\approx^{div}$
  - typically we have $|TS| \ll |TS/\approx^{div}|$
- $TS_1 \approx^{div} TS_2$ if and only if ($TS_1 \models \Phi$ iff $TS_2 \models \Phi$)
  - for any $\text{CTL}^*_{\setminus\bigcirc}$ (or $\text{CTL}_{\setminus\bigcirc}$) formula Φ

$\Rightarrow$ To check $TS \models \Phi$, if suffices to check whether $TS/\approx^{div} \models \Phi$

  - quotienting with respect to $\approx^{div}$ is a useful preprocessing step of model checking
  - quotienting can be used to determine whether $TS_1 \approx^{div} TS_2$

Approach

[Groote and Vaandrager, 1990]

1. A quotienting algorithm to determine $TS/\approx$:
   - remove *stutter cycles* from *TS*
   - a refine operator to *efficiently split* (blocks of) partitions
   - exploit partition-refinement (as for bisimulation $\sim$)

2. A quotienting algorithm to determine $TS/\approx^{div}$:
   - *transform* *TS* into a (divergence-sensitive) transition system $\overline{TS}$
   - $\overline{T}$ is divergent-sensitive, i.e., $\approx_{\overline{TS}}$ and $\approx^{div}_{\overline{TS}}$ coincide
   - determine $\overline{TS}/\approx$ using the quotienting algorithm for $\approx$
   - "distill" $TS/\approx^{div}$ from $\overline{TS}/\approx$

Stutter bisimulation

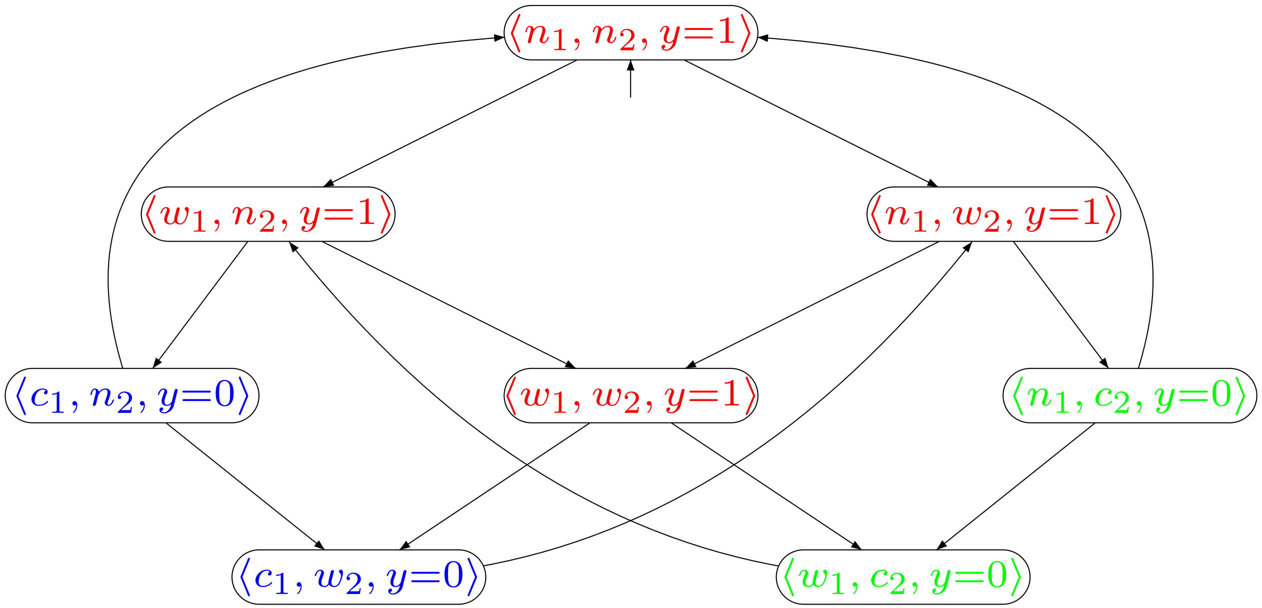
Let *TS* $= (S, \mathit{Act}, \rightarrow, I, \mathit{AP}, L)$ be a transition system and $\mathcal{R} \subseteq S \times S$

$\mathcal{R}$ is a *stutter-bisimulation* for *TS* if for all $(s_1, s_2) \in \mathcal{R}$:

1. $L(s_1) = L(s_2)$
2. if $s_1' \in \mathit{Post}(s_1)$ with $(s_1, s_1') \notin \mathcal{R}$, then there exists a finite path fragment $s_2 \, u_1 \, \ldots \, u_n \, s_2'$ with $n \geqslant 0$ and $(s_2, u_i) \in \mathcal{R}$ and $(s_1', s_2') \in \mathcal{R}$
3. if $s_2' \in \mathit{Post}(s_2)$ with $(s_2, s_2') \notin \mathcal{R}$, then there exists a finite path fragment $s_1 \, v_1 \, \ldots \, v_n \, s_1'$ with $n \geqslant 0$ and $(s_1, v_i) \in \mathcal{R}$ and $(s_1', s_2') \in \mathcal{R}$

s_1, s_2 are *stutter-bisimulation equivalent*, denoted $s_1 \approx_{\mathit{TS}} s_2$, if there exists a stutter bisimulation $\mathcal{R}$ for *TS* with $(s_1, s_2) \in \mathcal{R}$

Example



$\mathcal{R}$ inducing the following partitioning of the state space is a stutter bisimulation:

$$\{\{\langle n_1, n_2\rangle, \langle n_1, w_2\rangle, \langle w_1, n_2\rangle, \langle w_1, w_2\rangle\}, \{\langle c_1, n_2\rangle, \langle c_1, w_2\rangle\}, \{\langle c_2, n_1\rangle, \langle w_1, c_2\rangle\}\}$$

In fact, this is the coarsest stutter bisimulation, i.e., $\mathcal{R}$ equals $\approx_{TS}$

Quotient transition system

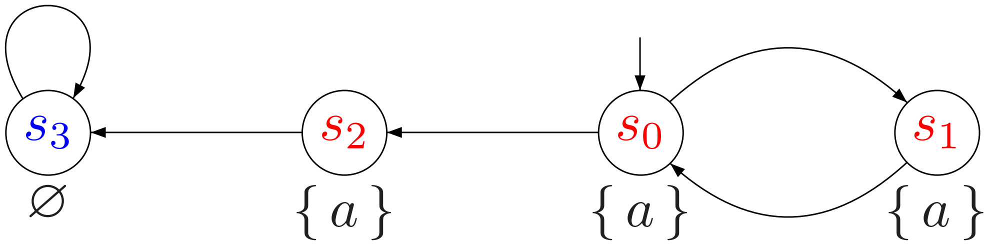
$$\mathit{TS}/\approx \, = \, (S', \{\tau\}, \rightarrow', I', \mathit{AP}, L'), \qquad \text{the } \textit{quotient} \text{ of } \mathit{TS} \text{ under } \approx$$

where

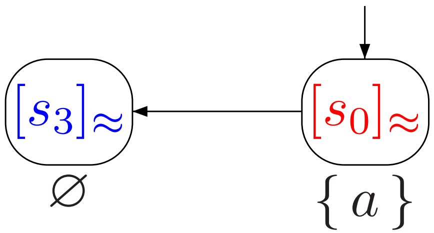
- $S' = S/\approx = \{ [s]_\approx \mid s \in S \}$
- $\rightarrow'$ is defined by: $$\frac{s \xrightarrow{\alpha} s' \text{ and } s \not\approx s'}{[s]_\approx \xrightarrow{\tau}{}' [s']_\approx}$$
- $I' = \{ [s]_\approx \mid s \in I \}$
- $L'([s]_\approx) = L(s)$

note that (a) no self-loops occur in $\mathit{TS}/\approx$ and (b) $\mathit{TS} \approx \mathit{TS}/\approx$

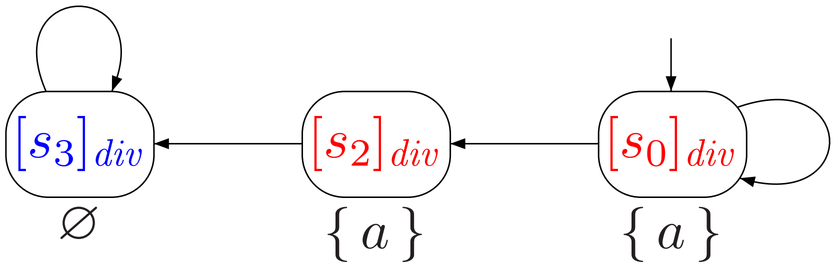
Example



transition system *TS*



transition system $TS/\approx$



transition system $TS/\approx^{div}$

Partition-refinement

from now on, we assume that *TS* is finite

- Iteratively compute a partition of S
- Initially: Π_0 equals $\Pi_{AP} = \{ (s,t) \in S \times S \mid L(s) = L(t) \}$ as before
- Repeat until no change: $\boxed{\Pi_{i+1} := \mathit{Refine}_{\approx}(\Pi_i)}$
  - loop invariant: Π_i is coarser than $S/\approx$ and finer than $\{ S \}$
- Return Π_i
  - termination: $\mathcal{R}_{\Pi_0} \supsetneqq \mathcal{R}_{\Pi_1} \supsetneqq \mathcal{R}_{\Pi_2} \supsetneqq \ldots \supsetneqq \mathcal{R}_{\Pi_i} = \approx_{TS}$
  - time complexity: maximally $|\,S\,|$ iterations needed

Theorem

$S/\approx$ is the *coarsest* partition Π of S such that:

(i) Π is finer than the initial partition Π_{AP}, and

(ii) $B \cap \mathit{Pre}(C) = \varnothing$ or $B \subseteq \mathit{Pre}^*_\Pi(C)$ for all $B, C \in \Pi$

$$s \in \mathit{Pre}^*_\Pi(C) \text{ whenever } \underbrace{s = s_1\, s_2 \ldots s_{n-1}}_{\in B}\ \underbrace{s_n}_{\in C} \in \mathit{Paths}(s)$$

state s can reach C via a path that is completely in B

The refinement operator

- Let: $\mathit{Refine}_{\approx}(\Pi, C) \;=\; \bigcup_{B \in \Pi} \mathit{Refine}_{\approx}(B, C)$ for C a block in Π
  - where $\mathit{Refine}_{\approx}(B, C) \;=\; \left\{ B \cap \mathit{Pre}^{*}_{\Pi}(C),\; B \setminus \mathit{Pre}^{*}_{\Pi}(C) \right\} \setminus \{ \varnothing \}$

- Basic properties:
  - for Π finer than Π_{AP} and coarser than $S/\approx$:

    $\mathit{Refine}_{\approx}(\Pi, C)$ is finer than Π and $\mathit{Refine}_{\approx}(\Pi, C)$ is coarser than $S/\approx$

  - Π is strictly coarser than $S/\approx$ if and only if there exists a *splitter* for Π

what is an appropriate splitter for $\approx$?

Splitter for $\approx$

Let Π be a partition of S and let C, $B \in \Pi$.

1. C is a Π-*splitter* for B if and only if:

$$B \neq C \quad \text{and} \quad B \cap \mathit{Pre}(C) \neq \varnothing \quad \text{and} \quad B \setminus \mathit{Pre}^*_\Pi(C) \neq \varnothing$$

2. Π is C-*stable* if there is no $B \in \Pi$ such that C is a Π-splitter for B

3. Π is *stable* if Π is C-stable for all blocks $C \in \Pi$

Partition-refinement

Input: finite transition system *TS* with state space S
Output: stutter-bisimulation quotient space $S/\approx$

$\Pi := \Pi_{AP}$; (* as before *)
while ($\exists B, C \in \Pi.\ C$ is a Π-splitter for B) **do**
choose such $B, C \in \Pi$;
$\Pi := (\Pi \setminus \{ B \}) \cup \{ \underbrace{B \cap Pre^*_\Pi(C)}_{B_1}, \underbrace{B \setminus Pre^*_\Pi(C)}_{B_2} \} \setminus \{ \varnothing \}$; (* refine Π *)
od
return Π

Removal of stutter cycles: Why?

- $s_0\, s_1\, \ldots s_n (= s_0)$ is a *stutter cycle* when $s_i\, s_{i+1}$ is a stutter step for $0 \leqslant i < n$
- For stutter cycle $s_0\, s_1\, s_2\, \ldots s_n$ in transition system *TS*:

$$s_0 \approx^{div}_{TS} s_1 \approx^{div}_{TS} \ldots \approx^{div}_{TS} s_n$$

- Corollary:

For finite transition system *TS* and state s in *TS*:

s is $\approx^{div}$ –divergent if and only if

a stutter cycle is reachable from s via a path in $[s]_{div}$

Removal of stutter cycles: How?

1. Determine the SCCs in $G(\mathit{TS})$ that only contain stutter steps
   - use depth-first search to find these strongly connected components (SCCs)
2. Collapse any stutter SCC into a single state
   - $C \rightarrow' C'$ with $C \neq C'$ whenever $s \rightarrow s'$ in *TS* with $s \in C$ and $s' \in C'$

$\Rightarrow$ Resulting TS' has no stutter cycles

- $s_1 \approx_{\mathit{TS}} s_2$ if and only if $\underbrace{C_1}_{s_1 \in C_1} \approx_{\mathit{TS}'} \underbrace{C_2}_{s_2 \in C_2}$

from now on, assume transition systems have no stutter cycles

Exit states

- C is a Π-*splitter* for B if and only if:

$$B \neq C \quad \text{and} \quad B \cap \mathit{Pre}(C) \neq \varnothing \quad \text{and} \quad B \setminus \mathit{Pre}^*_\Pi(C) \neq \varnothing$$

- How to avoid the computation of $\mathit{Pre}^*_\Pi(C)$ for $C \in \Pi$?
- No stutter cycles $\Rightarrow$ block $B \in \Pi$ has at least one *exit state*
  - exit state = a state with only direct successors outside B
  - $\mathit{exit}(B) = \left\{ s \in B \mid \mathit{Post}(s) \cap B = \varnothing \right\}$
- For finite *TS* without stutter cycles, C is a Π-*splitter* for B iff:

$$B \neq C \quad \text{and} \quad B \cap \mathit{Pre}(C) \neq \varnothing \quad \text{and} \quad \mathit{exit}(B) \setminus \mathit{Pre}(C) \neq \varnothing$$

Proof

Implementation details

Time complexity

For $\mathit{TS} = (S, \mathit{Act}, \rightarrow, I, \mathit{AP}, L)$ with $M \geqslant |S|$, the $\#$ edges in TS:

> The partition-refinement algorithm to compute $\mathit{TS}/\approx$
> has a worst-case time complexity in $\mathcal{O}\big(|S| \cdot (|\mathit{AP}| + M)\big)$

Approach

1. A quotienting algorithm to determine $TS/\approx$:

- remove *stutter cycles* from TS
- a refine operator to *efficiently split* (blocks of) partitions
- exploit partition-refinement (as for bisimulation $\sim$)

$\Rightarrow$ A quotienting algorithm to determine $TS/\approx^{div}$:

- *transform* TS into a (divergence-sensitive) transition system $\overline{TS}$
- $\overline{T}$ is divergent-sensitive, i.e., $\approx_{\overline{TS}}$ and $\approx^{div}_{\overline{TS}}$ coincide
- determine $\overline{TS}/\approx$ using the quotienting algorithm for $\approx$
- "distill" $TS/\approx^{div}$ from $\overline{TS}/\approx$

Divergence-sensitive stutter bisimulation

Let *TS* be a transition system and $\mathcal{R}$ an equivalence relation on S

- $\mathcal{R}$ is *divergence sensitive* if for any $(s_1, s_2) \in \mathcal{R}$:

$$s_1 \text{ is } \mathcal{R}\text{-divergent implies } s_2 \text{ is } \mathcal{R}\text{-divergent}$$

  - $\mathcal{R}$ is divergence-sensitive if in any $[s]_{\mathcal{R}}$ either all or none states are $\mathcal{R}$-divergent

- s_1, s_2 in *TS* are *divergent stutter-bisimilar*, denoted $s_1 \approx_{TS}^{div} s_2$, if:
  - $\exists$ divergent-sensitive stutter bisimulation $\mathcal{R}$ on *TS* such that $(s_1, s_2) \in \mathcal{R}$

Quotient transition system under $\approx^{div}$

$TS/\approx^{div} = (S', \{\tau\}, \rightarrow', I', AP, L')$, the *quotient* of *TS* under $\approx^{div}$

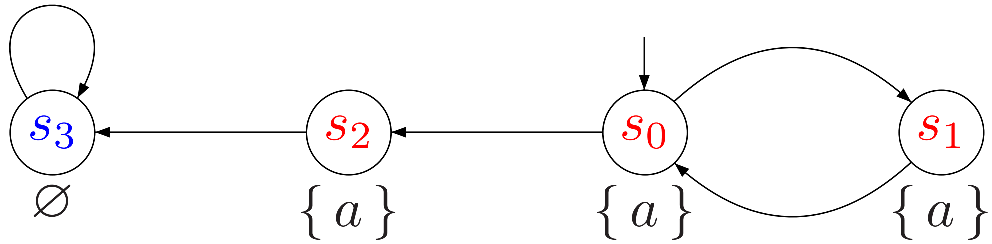
where

- S', I' and L' are defined as usual (for eq. classes $[s]_{div}$ under $\approx^{div}$)
- $\rightarrow'$ is defined by:

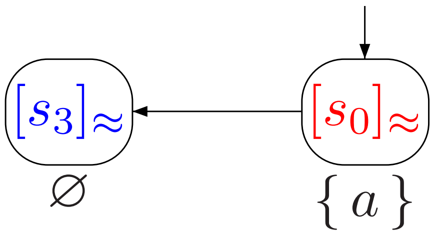
$$\frac{s \xrightarrow{\alpha} s' \ \wedge \ s \not\approx^{div} s'}{[s]_{div} \xrightarrow{\tau}'_{div} [s']_{div}} \quad \text{and} \quad \frac{s \text{ is } \approx^{div}\text{-divergent}}{[s]_{div} \xrightarrow{\tau}'_{div} [s]_{div}}$$

note that $TS \approx^{div} TS/\approx^{div}$

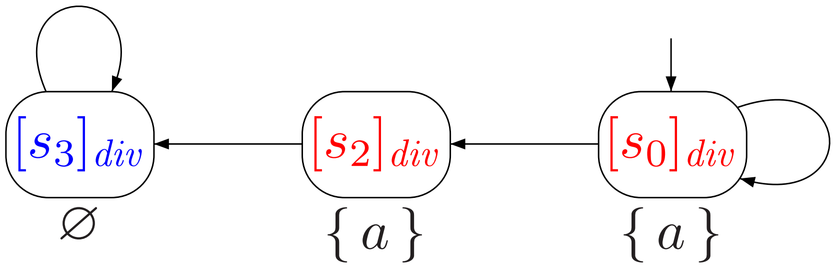
Example



transition system *TS*



transition system $TS/\approx$



transition system $TS/\approx^{div}$

Divergence expansion

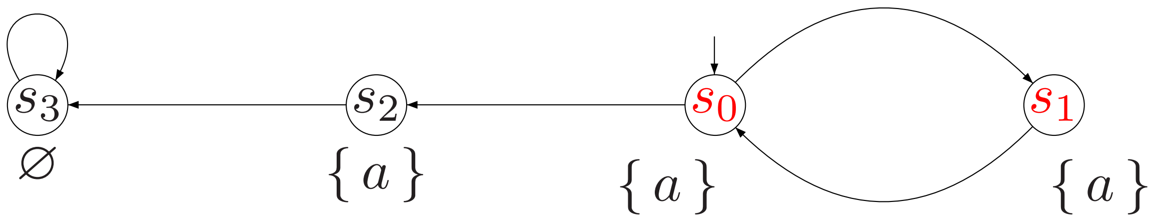
Divergence-sensitive expansion of finite $TS = (S, Act, \rightarrow, I, AP, L)$ is:

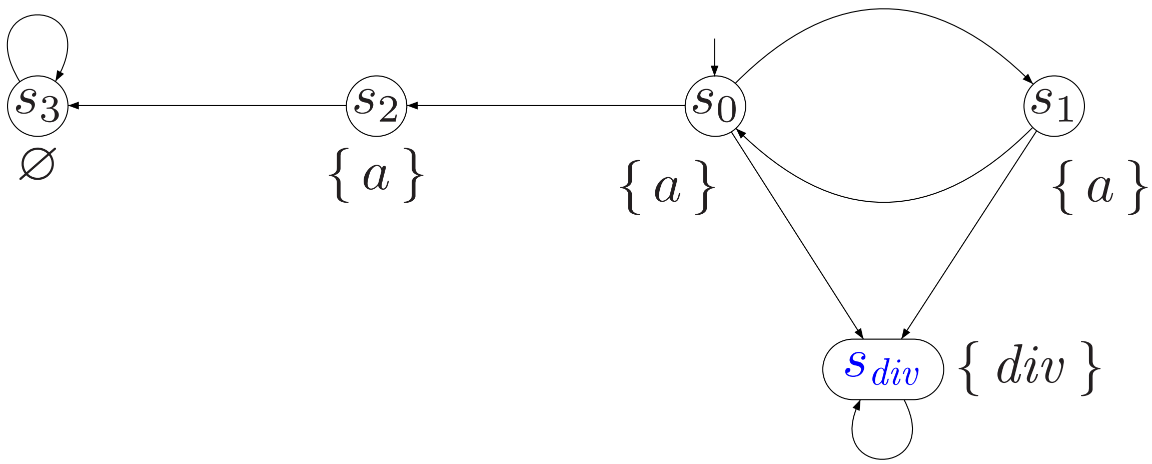
$$\overline{TS} = \big(S \cup \{ s_{div} \}, Act \cup \{ \tau \}, \rightarrow, I, AP \cup \{ div \}, \overline{L}\big) \quad \text{where}$$

- $s_{div} \notin S$
- $\rightarrow$ extends the transition relation of *TS* by:
  - $s_{div} \xrightarrow{\tau} s_{div}$ and
  - $s \xrightarrow{\tau} s_{div}$ for every state $s \in S$ on a stutter cycle in *TS*
- $\overline{L}(s) = L(s)$ if $s \in S$ and $\overline{L}(s_{div}) = \{ div \}$

$s_{div} \not\approx s$ for any $s \in S$ and s_{div} can only be reached from a $\approx^{div}$-divergent state

Example





Correctness

For finite transition system *TS*:

1. $\overline{TS}$ is divergence-sensitive, and

2. for all $s_1, s_2 \in S$: $s_1 \approx^{div}_{TS} s_2$ if and only if $s_1 \approx_{\overline{TS}} s_2$

Proof

Recipe for computing $\mathit{TS}/\approx^{div}$

1. Construct the divergence-sensitive expansion $\overline{\mathit{TS}}$
   - determine the SCCs in $G_{stutter}(\mathit{TS})$, and insert transitions $s_{div} \longrightarrow s_{div}$ and
   - $s \longrightarrow s_{div}$ for any state s in a non-trivial SCC of $G_{stutter}$
2. Apply partition-refinement to $\overline{\mathit{TS}}$ to obtain $S/\approx^{div}_{\mathit{TS}} \; = \; S/\approx_{\overline{\mathit{TS}}}$
3. Generate $\overline{\mathit{TS}}/\approx$
   - any $C \in S/\approx^{div}$ that contains an initial state of TS is an initial state
   - the labeling of $C \in S/\approx^{div}$ equals the labeling of any $s \in C$
   - any transition $s \longrightarrow s'$ with $s \not\approx^{div}_{\mathit{TS}} s'$ yields a transition between C_s and $C_{s'}$
4. "Distill" $\mathit{TS}\approx^{div}$ from $\overline{\mathit{TS}}/\approx$:
   - replace transition $s \longrightarrow s_{div}$ in $\overline{\mathit{TS}}$ by the self-loop $[s]_{div} \longrightarrow [s]_{div}$
   - delete state s_{div}

Example

Time complexity

For *TS* $= (S, \textit{Act}, \rightarrow, I, \textit{AP}, L)$ with $M \geqslant |S|$, the $\#$ edges in *TS*:

The quotient transition system *TS*$/\approx^{div}$ can be determined with a worst-case time complexity in $\mathcal{O}\big(|S|+M \ + \ |S| \cdot (|\textit{AP}|+M)\big)$