Simulation and bisimulation

(IF311 : "Formal methods in software design")

Frédéric Herbreteau (fh@labri.fr)

Bordeaux INP

Motivation

Big models are out of the scope of model-checking:

- variables that range over **huge domains** (32-bits integers, ...)
- variables that are **unbounded** (integers $\mathbb{N}, \mathbb{Z}$, arrays $[0, n] \to E$ for $n \in \mathbb{N}$, ...)

Goal: build an **abstract** model that allows to prove the **actual** algorithm

Plan

Simulation

Bisimulation

Quotient

Property preservation

Simulation relation

Let $T_1 = (S_1, S_{01}, \rightarrow_1, L_1)$ and $T_2 = (S_2, S_{02}, \rightarrow_2, L_2)$ be two transition systems.

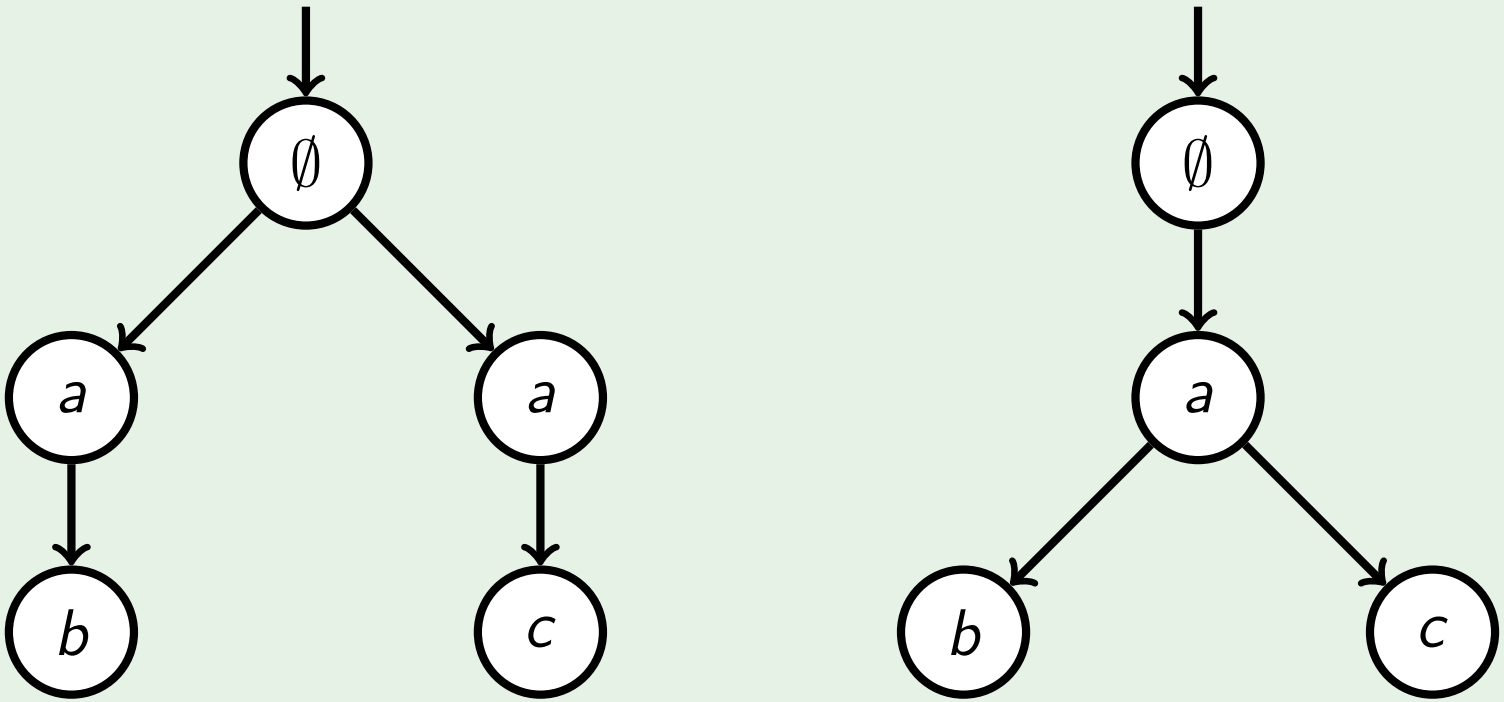
Definition

A relation $R \subseteq S_1 \times S_2$ is a **simulation relation** if:

- for each $s_1 \in S_{01}$ there exists $s_2 \in S_{02}$ s.t. $(s_1, s_2) \in R$,
- for every $(s_1, s_2) \in R$:
  - $L_1(s_1) = L_2(s_2)$,
  - and for every s_1' such that $s_1 \rightarrow_1 s_1'$, there exists s_2' such that $s_2 \rightarrow_2 s_2'$ and $(s_1', s_2') \in R$

Illustration

Example



- Simulation relations between these two transition systems?

Simulation relations preserve reachability

Theorem

If $T_1 \preceq T_2$ and $s_1 \in S_1$ is reachable, there exists $s_2 \in S_2$ such that s_2 is reachable and s_1 is simulated by s_2.

Proof.

Exercise □

Example

Consequences of the last theorem on **non-reachability** properties (assertions)?

Plan

Simulation

Bisimulation

Quotient

Property preservation

Bisimulation relation

Definition

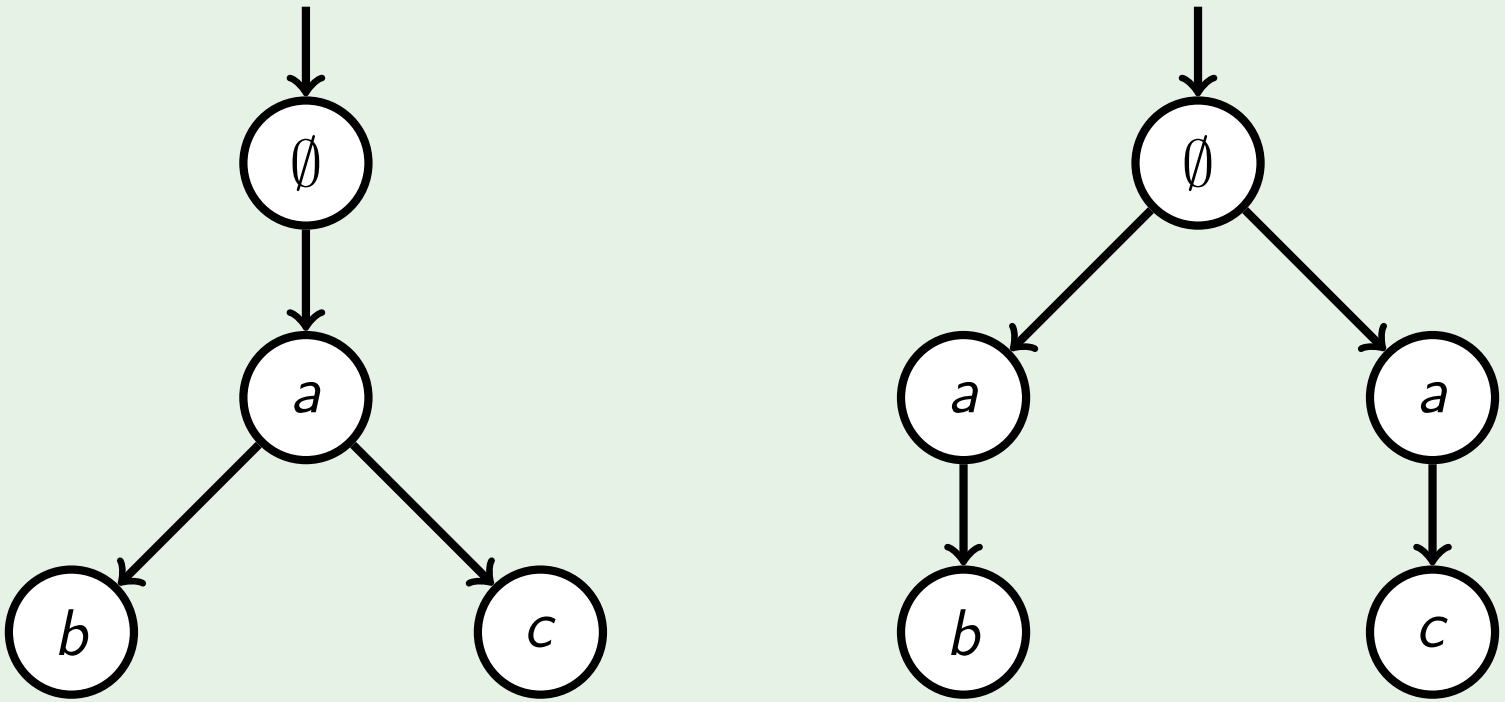
A relation $R \subseteq S_1 \times S_2$ is a **bisimulation relation** if both R and R^{-1} are simulation relations.

$$\begin{array}{ccc} s_1 & R & s_2 \\ \forall \downarrow & & \downarrow \exists \\ s_1' & R & s_2' \end{array} \quad \text{and} \quad \begin{array}{ccc} s_1 & R & s_2 \\ \exists \downarrow & & \downarrow \forall \\ s_1' & R & s_2' \end{array}$$

We denote $T_1 \simeq T_2$ "T_1 and T_2 are bisimilar" if there exists a bisimulation relation R as above.

Illustration 1

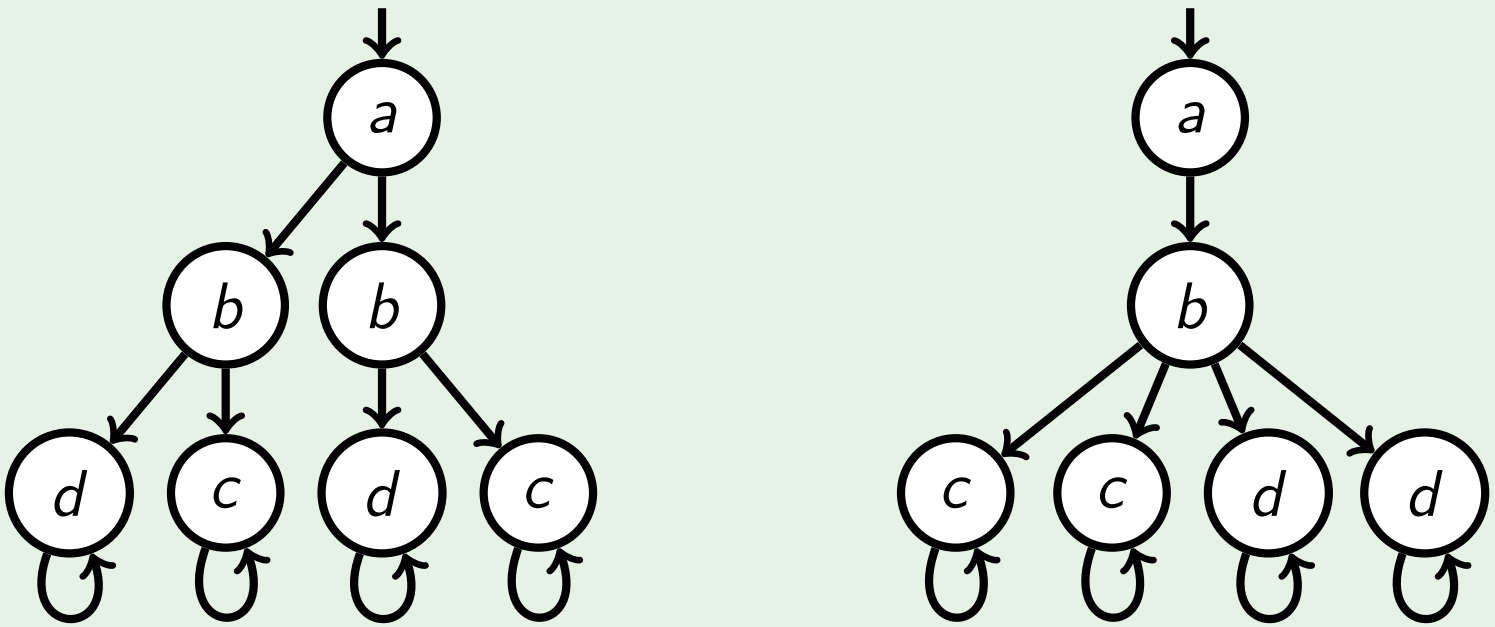
Example



- Bisimulation relation between these two transition systems?

Illustration 2

Example



- Bisimulation relation between these two transition systems?

Plan

Quotient (existential abstraction)

Let T be a transition system and $R \subseteq S \times S$ be an **equivalence relation** on the states of T.

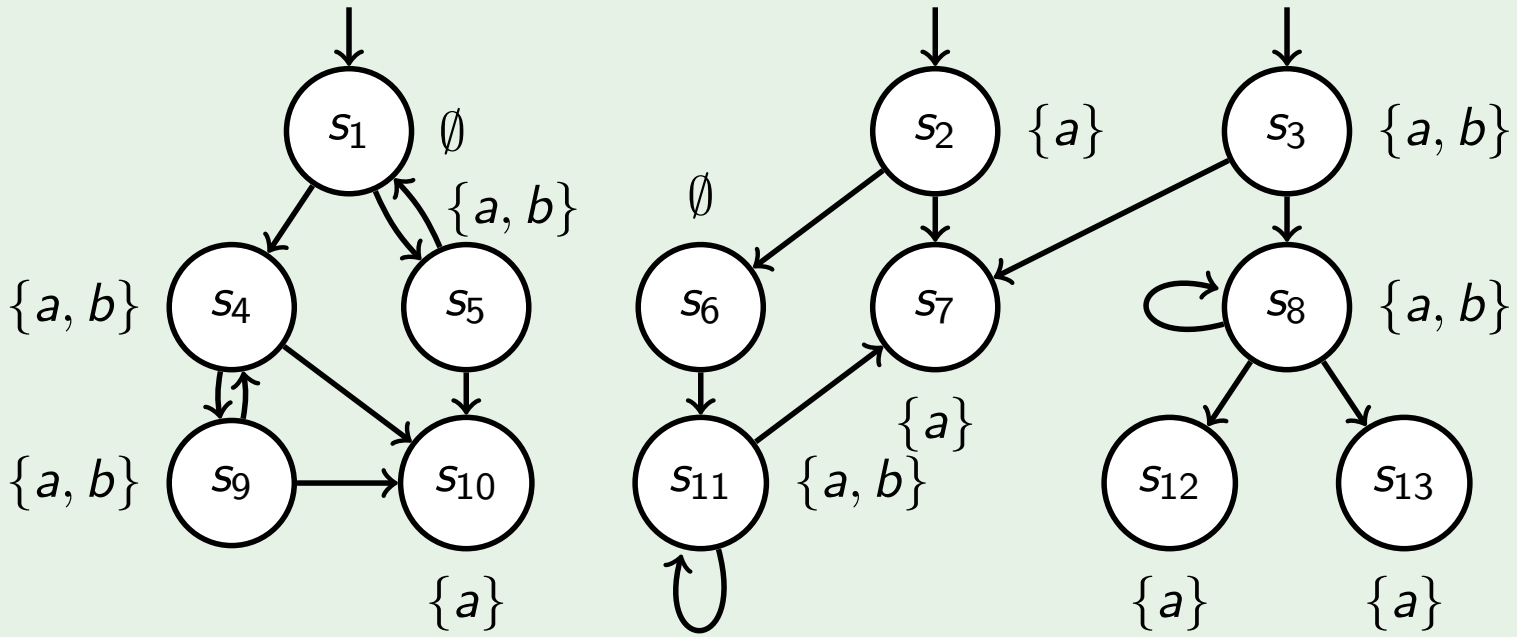
Definition

The **quotient** $\widehat{T_R}$ of T by R is the transition system $(\widehat{S}, \widehat{S_0}, \rightsquigarrow, \widehat{L})$ defined by:

- $\widehat{S}$ are the equivalence classes of R;
- $\widehat{S_0}$ is the equivalence class of S_0;
- $X \overset{a}{\rightsquigarrow} X'$ iff **there exists** $s \in X$ and $s' \in X'$ s.t. $s \overset{a}{\rightarrow} s'$;
- $\widehat{L}(X)$ is the union of $L(s)$ for $s \in X$.

Illustration

Example



- Determine a bisimulation equivalence R on the states of transition system T above.
- Compute the quotient of T by R

Plan

Simulation

Bisimulation

Quotient

Property preservation

Property preservations for simulations

Theorem

If $T_1 \preceq T_2$, then for every LTL property Φ, $T_2 \models \Phi$ implies $T_1 \models \Phi$.

Theorem

Simulation relations do not preserve deadlocks.

Theorem

If R is a simulation relation over T, then $T \preceq \widehat{T_R}$

Proof.

Exercises $\square$

Property preservations for bisimulations

Theorem

If $T_1 \simeq T_2$, then for every LTL property Φ, $T_2 \models \Phi$ iff $T_1 \models \Phi$.

Theorem

Bisimulation relations preserve deadlocks.

Theorem

If R is a bisimulation relation over T, then $T \simeq \widehat{T_R}$

Proof.

Exercises □