Model Checking I
alias
Reactive Systems Verification

Luca Tesei

MSc in Computer Science, University of Camerino

Topics

- Parallelism
- Interleaving operator for Transition Systems
- Examples

Material

Reading:

Chapter 2 of the book, pages 35–39.

More:

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

Overview

Parallelism and communication

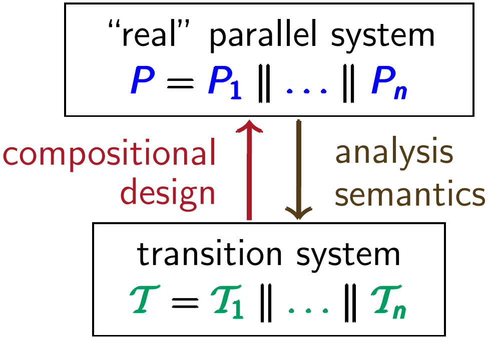
"real" parallel system

$P = P_1 \parallel \ldots \parallel P_n$

transition system

$\mathcal{T} = \mathcal{T}_1 \parallel \ldots \parallel \mathcal{T}_n$

Parallelism and communication



Parallelism and communication

"real" parallel system

$$P = P_1 \parallel \ldots \parallel P_n$$

compositional design ↑ ↓ analysis semantics

transition system

$$\mathcal{T} = \mathcal{T}_1 \parallel \ldots \parallel \mathcal{T}_n$$

goal: define semantic parallel operators on transition systems or program graphs that model "real" parallel operators

Interleaving operator $|||$ for TS

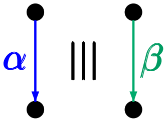
- interleaving of concurrent, independent actions of parallel processes (modelled by TS)
- representation by nondeterministic choice:
  "which subprocess performs the next step?"

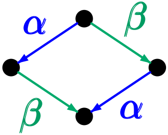
Interleaving operator ||| for TS

- interleaving of concurrent, independent actions of parallel processes (modelled by TS)
- representation by nondeterministic choice:

  "which subprocess performs the next step?"

$$\mathit{effect}(\alpha|||\beta) \;=\; \mathit{effect}(\alpha;\beta+\beta;\alpha)$$

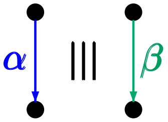


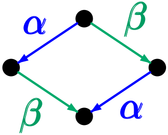


Interleaving operator ||| for TS

- interleaving of concurrent, independent actions of parallel processes (modelled by TS)
- representation by nondeterministic choice:
  "which subprocess performs the next step?"

$$\mathit{effect}(\alpha|||\beta) \;=\; \mathit{effect}(\alpha;\beta+\beta;\alpha)$$

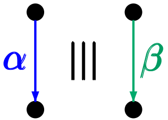


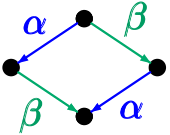


parallel execution
of α and β on
two processors

- interleaving of concurrent, independent actions of parallel processes (modelled by TS)
- representation by nondeterministic choice:
  "which subprocess performs the next step?"

$$effect(\alpha|||\beta) \;=\; effect(\alpha;\beta+\beta;\alpha)$$





parallel execution of α and β on *two processors* $\widehat{=}$ serial execution on a *single processor* in arbitrary order

Interleaving operator $|||$ for TS

$$\mathcal{T}_1 = (S_1, Act_1, \longrightarrow_1, S_{0,1}, AP_1, L_1)$$
$$\mathcal{T}_2 = (S_2, Act_2, \longrightarrow_2, S_{0,2}, AP_2, L_2)$$

Interleaving operator ||| for TS

$$\mathcal{T}_1 \;=\; (S_1, Act_1, \longrightarrow_1, S_{0,1}, AP_1, L_1)$$

$$\mathcal{T}_2 \;=\; (S_2, Act_2, \longrightarrow_2, S_{0,2}, AP_2, L_2)$$

The transition system $\mathcal{T}_1 \,|||\, \mathcal{T}_2$ is defined by:

$$\mathcal{T}_1 \,|||\, \mathcal{T}_2 = (S_1 \times S_2, Act_1 \cup Act_2, \longrightarrow, S_{0,1} \times S_{0,2}, AP, L)$$

where the transition relation $\longrightarrow$ is given by:

Interleaving operator $|||$ for TS

$$\mathcal{T}_1 \;=\; (S_1, Act_1, \longrightarrow_1, S_{0,1}, AP_1, L_1)$$

$$\mathcal{T}_2 \;=\; (S_2, Act_2, \longrightarrow_2, S_{0,2}, AP_2, L_2)$$

The transition system $\mathcal{T}_1 \,|||\, \mathcal{T}_2$ is defined by:

$$\mathcal{T}_1 \,|||\, \mathcal{T}_2 = (S_1 \times S_2, Act_1 \cup Act_2, \longrightarrow, S_{0,1} \times S_{0,2}, AP, L)$$

where the transition relation $\longrightarrow$ is given by:

$$\frac{s_1 \xrightarrow{\alpha}_1 s_1'}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1', s_2 \rangle} \qquad \frac{s_2 \xrightarrow{\alpha}_2 s_2'}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1, s_2' \rangle}$$

Interleaving operator ||| for TS

$$\mathcal{T}_1 = (S_1, Act_1, \longrightarrow_1, S_{0,1}, AP_1, L_1)$$

$$\mathcal{T}_2 = (S_2, Act_2, \longrightarrow_2, S_{0,2}, AP_2, L_2)$$

The transition system $\mathcal{T}_1 \,|||\, \mathcal{T}_2$ is defined by:

$$\mathcal{T}_1 \,|||\, \mathcal{T}_2 = (S_1 \times S_2, Act_1 \cup Act_2, \longrightarrow, S_{0,1} \times S_{0,2}, AP, L)$$

where the transition relation $\longrightarrow$ is given by:

$$\frac{s_1 \xrightarrow{\alpha}_1 s_1'}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1', s_2 \rangle} \qquad \frac{s_2 \xrightarrow{\alpha}_2 s_2'}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1, s_2' \rangle}$$

atomic propositions: $AP = AP_1 \uplus AP_2$

labeling function: $L(\langle s_1, s_2 \rangle) = L_1(s_1) \cup L_2(s_2)$

SOS-notation (structured operational semantics)

just a simple notation for operational semantics

$$\frac{\textbf{premise}}{\textbf{conclusion}}$$

just a simple notation for operational semantics

$$\frac{\textbf{premise}}{\textbf{conclusion}}$$

E.g., *"the relation $\longrightarrow$ is given by ..."*

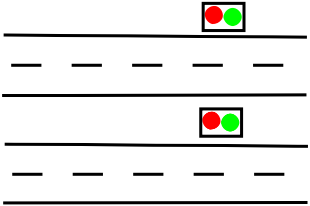
$$\frac{s_1 \xrightarrow{\alpha}_1 s_1'}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1', s_2 \rangle} \qquad \frac{s_2 \xrightarrow{\alpha}_2 s_2'}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1, s_2' \rangle}$$

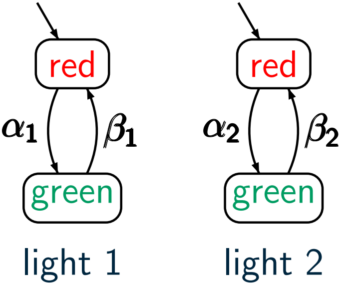
means that $\longrightarrow$ is the smallest relation such that:

(1) If $s_1 \xrightarrow{\alpha}_1 s_1'$, then $\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1', s_2 \rangle$

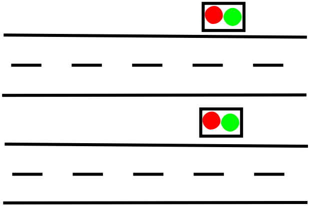
(2) If $s_2 \xrightarrow{\alpha}_2 s_2'$, then $\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1, s_2' \rangle$

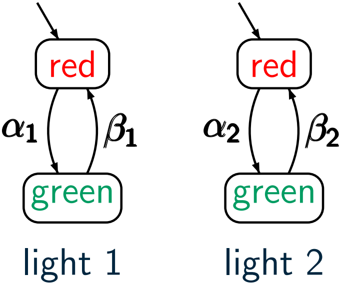
Useless lights for non-crossing streets



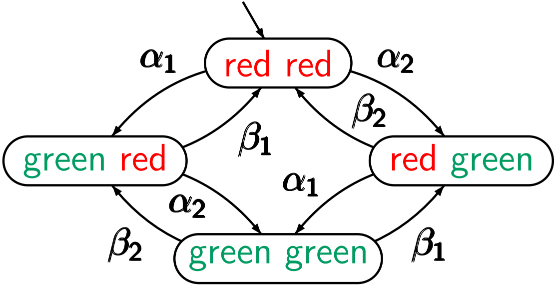


Useless lights for non-crossing streets





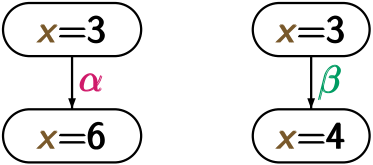
light 1 ||| light 2



Dependent actions

dependent actions $\alpha \mathrel{\widehat{=}} x{:=}2x$ and $\beta \mathrel{\widehat{=}} x{:=}x+1$

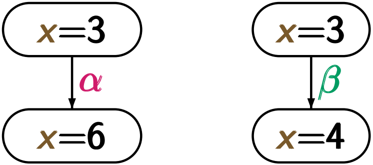
representations in transition systems



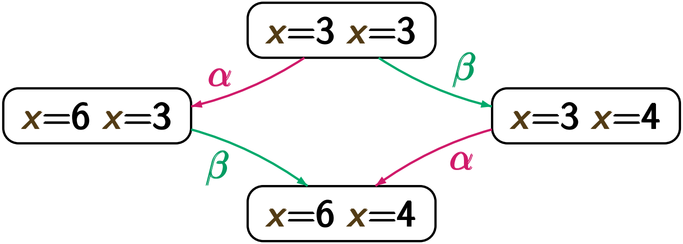
Dependent actions

dependent actions $\alpha \mathrel{\widehat{=}} x{:=}2x$ and $\beta \mathrel{\widehat{=}} x{:=}x{+}1$

representations in transition systems

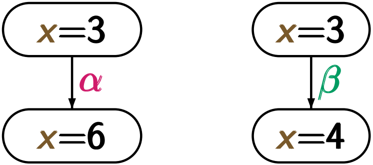


interleaving operator $|||$

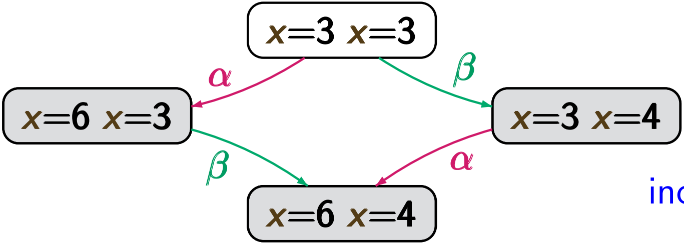


dependent actions $\alpha \mathrel{\widehat{=}} x{:=}2x$ and $\beta \mathrel{\widehat{=}} x{:=}x+1$

representations in transition systems



interleaving operator ||| for transition systems "fails"



inconsistent states