Prof. Dr. A. Podelski,
Dr. B. Westphal
M. Steinle

Summer term 2020

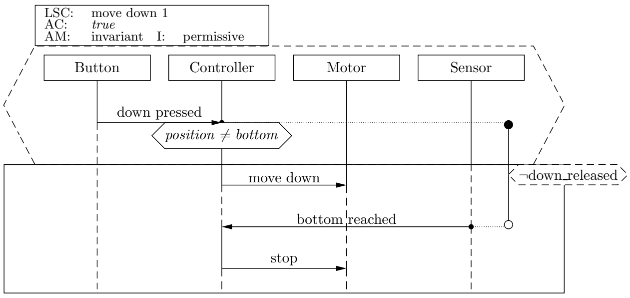
Softwaretechnik/Software Engineering

http://swt.informatik.uni-freiburg.de/teaching/SS2020/swtvl

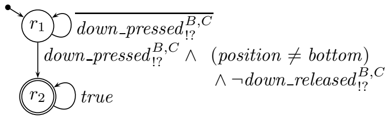
Exercise Sheet 2

Early submission: Monday, 2020-06-08, 14:00 Regular submission: Tuesday, 2020-06-09, 14:00

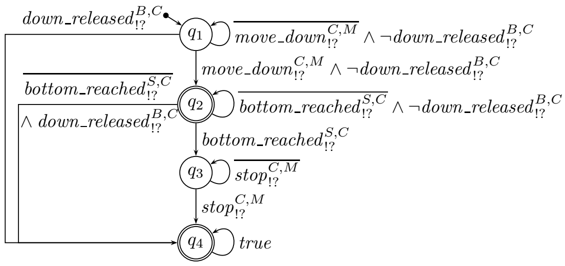
Exercise 1 – Validating LSC Specifications (5/20 Points)



(a) LSC 'move down 1'.



(b) Pre-chart TBA of 'move down 1'.



(c) Main-chart TBA of 'move down 1'.

Figure 1: Powerwindow specification.

Consider the LSC requirements specification for a power window in Figure 1a and the TBAs of pre- and main-chart given in Figures 1b and 1c. For the following computation paths, state whether it *trivially satisfies* (main-chart not activated), *non-trivially satisfies with legal exit* or *without* (in *complete* or *partial* traversal, i.e., final state reached or not), or *violates* the LSC, where the violation can be due to *violated condition*, *violated progress condition*, or *either message sending or reception missing* and argue your claim with the TBAs.
All computation paths end in an infinite sequence of τ-transitions (they 'do not do anything' after the last given transition). We use the following abbreviations: p/position, bot/bottom, up/up_pressed, dp/down_pressed, dr/down_released, md/move_down, br/bottom_reached, st/stop.

(i) $$\pi_1 \equiv \sigma_0 \xrightarrow{\tau} \underset{(p=bot)}{\sigma_1} \xrightarrow{up^{B,C}_{!?}} \underset{(p=bot)}{\sigma_2} \xrightarrow{\tau} \cdots \quad (1)$$

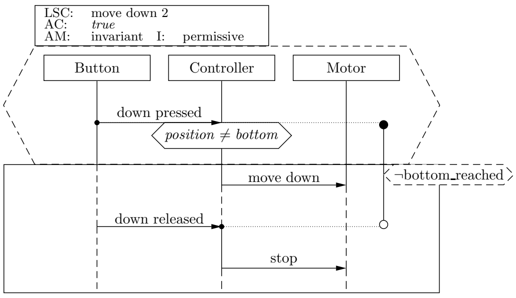
(ii) $$\pi_2 \equiv \sigma_0 \xrightarrow{\tau} \underset{(p\neq bot)}{\sigma_1} \xrightarrow{dp^{B,C}_{!?}} \sigma_2 \xrightarrow{\tau} \sigma_3 \xrightarrow{md^{C,M}_{!?}} \sigma_4 \xrightarrow{\tau} \cdots \quad (1)$$

(iii) $$\pi_3 \equiv \sigma_0 \xrightarrow{\tau} \underset{(p\neq bot)}{\sigma_1} \xrightarrow{dp^{B,C}_{!?}} \sigma_2 \xrightarrow{\tau} \sigma_3 \xrightarrow{md^{C,M}_{!?}} \sigma_4 \xrightarrow{br^{S,C}_{!?}} \sigma_5 \xrightarrow{\tau} \cdots \quad (1)$$

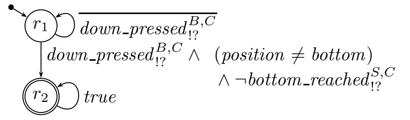
(iv) $$\pi_4 \equiv \sigma_0 \xrightarrow{\tau} \underset{(p\neq bot)}{\sigma_1} \xrightarrow{dp^{B,C}_{!?}} \sigma_2 \xrightarrow{\tau} \sigma_3 \xrightarrow{md^{C,M}_{!?}} \sigma_4 \xrightarrow{br^{S,C}_{!?}} \sigma_5 \xrightarrow{st^{C,M}_{!?}} \sigma_6 \xrightarrow{\tau} \cdots \quad (1)$$

(v) $$\pi_5 \equiv \sigma_0 \xrightarrow{\tau} \underset{(p\neq bot)}{\sigma_1} \xrightarrow{dp^{B,C}_{!?}} \sigma_2 \xrightarrow{\tau} \sigma_3 \xrightarrow{md^{C,M}_{!?}} \sigma_4 \xrightarrow{dr^{B,C}_{!?}} \sigma_5 \xrightarrow{st^{C,M}_{!?}} \sigma_6 \xrightarrow{\tau} \cdots \quad (1)$$

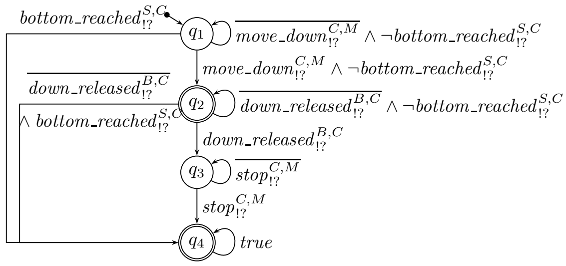
Exercise 2 – Validating LSC Specifications Continued (5 Bonus)



(a) LSC 'move down 2'.



(b) Pre-chart TBA of 'move down 2'.



(c) Main-chart TBA of 'move down 2'.

Figure 2: Powerwindow specification continued.

Figure 2 gives a second LSC requirements specification for the same power window.

(i) Does computation path π_5 satisfy or violate (trivial, non-trivial, etc.) Figure 2a? Argue your statement on the TBAs. (1)

(ii) Discuss the following computation path wrt. both LSC.

$$\pi_6 \equiv \sigma_0 \xrightarrow{\tau} \underset{(p \neq bot)}{\sigma_1} \xrightarrow{dp^{B,C}_{!?}} \sigma_2 \xrightarrow{\tau} \sigma_3 \xrightarrow{md^{C,M}_{!?}} \sigma_4 \xrightarrow{br^{S,C}_{!?}, dr^{B,C}_{!?}} \sigma_5 \xrightarrow{st^{C,M}_{!?}} \sigma_6 \xrightarrow{\tau} \cdots \quad (2)$$

(iii) Could a power window system on which we can observe computation paths π_5 and π_6 satisfy the overall specification consisting of the LSCs in Figures 1a and 2a? Should it? (2)

Exercise 3 – LSC Syntax (5/20 Points)

To investigate the semantics of the LSC shown in Figure 3, we need its **abstract syntax**.

(i) Provide the set of locations $\mathcal{L}$ including their temperature (make sure to clearly indicate where in the diagram which of your locations occurs). (2)

(ii) Give the partial order relation $\preceq$ on the locations (only direct predecessors/successors need to be given; the full relation $\preceq$ is then the transitive, reflexive closure). (2)

(iii) Give one example each of (a) an element of the simultaneity relation $\sim$, (b) a message from Msg (including temperature), (c) a local invariant from LocInv (including temperature), and (d) a condition from Cond (including temperature). (1)

Use the formal notations from the lecture; you can indicate the temperature with colors.

Hint: Note that all locations in a coregion obtain the same temperature from the relevant instance line segment adjacent to the whole coregion.

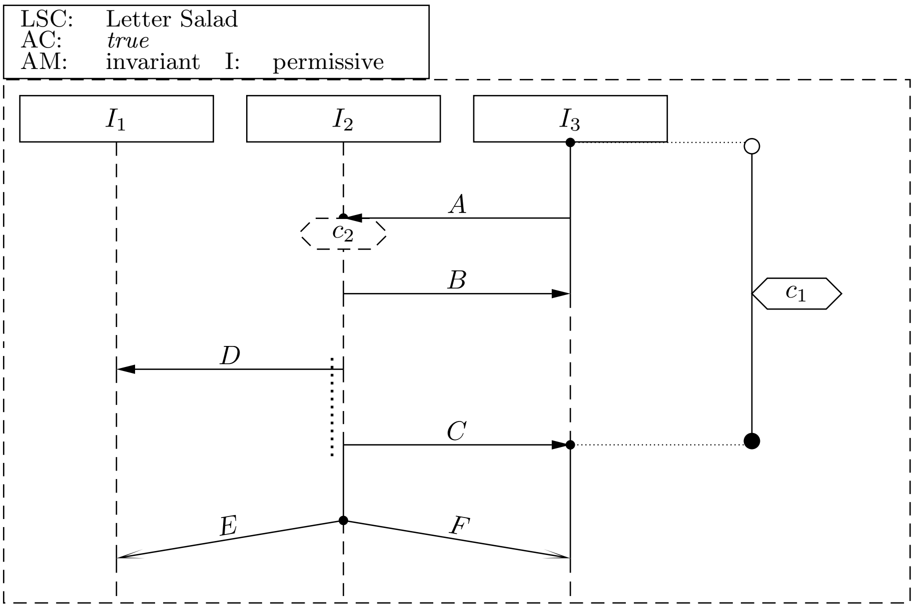


Figure 3: A Live Sequence Chart.

Exercise 4 – LSC Semantics (5/20 Points)

(i) Give the cuts (including their temperatures) and corresponding fired sets for the body of the chart in Figure 3.
For at least one hot and cold cut prove why they are hot/cold. (2)

(ii) Compute the Büchi automaton for the body of the chart in Figure 3. (2)

(iii) Provide the strictness conditions ψ_{strict} for one progress transition. (1)

Exercise 5 – LSC Acceptance (3/20 Points)

(i) Consider the following computation path π_1.

$$\pi_1 \equiv \sigma_0 \xrightarrow{A_!^{I_3,I_2} \wedge A_?^{I_3,I_2}} \sigma_1 \xrightarrow{B_!^{I_2,I_3} \wedge B_?^{I_2,I_3}} \sigma_2 \xrightarrow{\tau} \sigma_3 \xrightarrow{\tau} \cdots$$

where $\sigma_i \models c_1 \wedge \neg c_2$ for all $i \geq 0$.

Intuitively, the first event in the path is sending and receiving the message A. The second event is sending and receiving the message B. After that, no event happens ever again. During the whole computation path the condition c_1 holds and the condition c_2 is violated.

Is the path π_1 accepted by the chart or does it violate the chart? If it is accepted, does it take a legal exit or not? (1)

(ii) Give two further **computation paths** π_2 and π_3 such that each of the following conditions is satisfied by one of the paths π_1, π_2, or π_3:

- One of the paths violates the chart.
- One of the paths is accepted and takes a legal exit.
- One of the paths is accepted without taking a legal exit.

Use π_1, π_2, and π_3 to explain in your own words the intuition behind the concepts of acceptance with and without taking a 'legal exit', and of violation of a chart. (2)

Exercise 6 – Use Cases and Use Case Diagrams (2/20 Points)

name	exercise submission (preliminaries)
goal	exercise sheet solution uploaded
precondition	student navigated to exercise group screen in ILIAS
postcondition	student has submitted their solutions
actors	student (main actor), tutor
open questions	none
normal case	1. student opens the current exercise sheet tab 2. Ilias shows 'Hand In' button 3. student clicks 'Hand In' button
exception case 1a	submission deadline exceeded 2a.1 Ilias does not show 'Hand In' button due to deadline 2a.2 student sends solutions to tutor via e-mail and explains why the submission is late

Figure 4: Example Use Case.

(i) Provide the *use case diagram* for the simple use case in Figure 4. (1)

Hint: As usual, convince your tutor of the correctness of your solution.

(ii) Why is Task (i) only worth one single, lonely exercise point? (1)