Reactive Systems: Modelling, Specification and Verification
ERRATA

September 9, 2014

Please, send any errors and typos you might discover while reading the book to

`rsbook@cs.aau.dk`.

If possible, include the page and line number (e.g. page 12, line 6) and describe briefly the error.

- page 14, line 10: The expression "labelled transition" is mistakenly repeated.
  Thanks to Ahmed Khademzadeh.

- page 19, Definition 2.1: Denoting the transition relation as a set of binary relations is formally not completely ok as if e.g. for two different actions the corresponding binary relations are equal, this will not be correctly represented as a set. It should be instead an indexed family of relations $(\xrightarrow{\alpha})_{\alpha \in Act}$.
  Thanks to Christoph Wagner and Uwe Nestmann.

- page 22, add a third condition on relabelling function saying: $f(a) \neq \tau$ for each label a. This condition is indirectly implied by the second condition and the fact that $\overline{\tau}$ is undefined but an explicit formulation can make this fact clearer.
  Thanks to Søren Enevoldsen.

- page 20, last line in Exercise 2.4: The question mark should be replaced with a full stop.
  Thanks to Bertrand Dechoux.

- page 22, line 19: the set L of labels should be from $\mathcal{A}$ and not $\mathcal{L}$.

- page 30, Exercise 2.13: The introduction of the linking operator is now described in more detail in a note available as Supplementary Reading on the book's homepage: `http://www.cs.aau.dk/rsbook`.

- page 33, ll. 12–14 of the text: This paragraph was modified by the copy editor and the typesetters at CUP. The original text read:

  > This means that process descriptions that are related by R can be used interchangeably as parts of a larger process description without affecting its overall behaviour.

  Thanks to Petr Jančar.

- page 55, Figure 3.3: The comma in Good $\equiv (\overline{\text{coffee}}, \text{CM}_b \mid \ldots)$ should be an action prefixing like Good $\equiv (\overline{\text{coffee}}.\text{CM}_b \mid \ldots)$
  Thanks to Steinar Hugi Sigurdarson.

- page 70, Exercise 3.39, lines 5–6: The definition of 2-nested simulation is wrong, in fact, it defines bisimulation as $\mathcal{R}^{-1} \subseteq \mathcal{R}$ implies that $\mathcal{R}$ is symmetric. The correct formulation is:

  > A binary relation $\mathcal{R}$ over the set of states of an LTS is a 2-nested simulation iff $\mathcal{R}$ is a simulation and there is some relation of simulation $\mathcal{R}'$ such that $\mathcal{R}^{-1} \subseteq \mathcal{R}'$.

  Thanks to Petr Jančar.

- page 76, Example 4.1, 4th bullet: The second item in the formal definition of the lexicographic order is incorrect, as it gives rise to a relation that is not antisymmetric. The definition of the lexicographic order should read as follows.

  > Recall that, for all $s, t \in A^*$, the relation $s \prec t$ holds with respect to the lexicographic order if one of the following conditions apply:
  >
  > 1. $s = t$;
  > 2. the length of s is smaller than that of t;
  > 3. s and t have equal length, and either $s = \varepsilon$ or there are strings $u, v, z \in A^*$ and letters $a, b \in A$ such that $s = uav$, $t = ubz$ and $a < b$.

  Thanks to Petr Jančar.

- page 76, Example 4.1, 4th bullet: The notion of lexicographic order we have defined above is non-standard, and should be compared with the one presented at, e.g., `http://en.wikipedia.org/wiki/Lexicographical_order`.
  Thanks to Roberto Gorrieri.

- page 78, Example 4.2, line -3: Replace "$\leq$" with "$\sqsubseteq$".
  Thanks to Roberto Gorrieri.

- page 81, line 15: "$f : S \to S$." should read "$f : 2^S \to 2^S$."
  Thanks to Arnar Birgisson.

- page 94, line 5: It would be more precise to write "can always have a biscuit" instead of "must always have a biscuit"
  Thanks to Roberto Gorrieri.

- page 98, line 16: We should add to the claim "However, all the other processes that we have met so far in this text are image finite." that this is except those in Section 2.2.3 where a variable x appears free in the process P.
  Thanks to Uwe Nestmann.

- page 121, l. -16: variabls → variable.
  Thanks to Petr Jančar.

- page 133, line -1: "$q \in [p']_\sim$" should read "$q' \in [p']_\sim$"
  Thanks to Arnar Birgisson.

- page 138, line -3: Rooted LTS has not been defined. Instead, the text should say: "Next, construct an LTS toghether with a state that satisfies the property and one that does not."
  Thanks to Uli Fahrenberg.

- page 146, Exercise 7.3, line 10: The while condition $k \neq j$ in Hyman's algorithm should read as $k \neq i$.
  Thanks to Petr Jančar.

- page 152, lines 12–13: Contrary to what we claimed in the book, the command `pre` offered by the CWB does *not* check for the existence of a weak simulation between its arguments. Rather, it checks for the existence of a weak prebisimulation in the sense of the paper:

  D.J. Walker. Bisimulation and divergence, Information and Computation 85(2):202–241, 1990.

  To check that some process Q weakly simulates P using the command `pre` offered the CWB, it suffices to issue the command `pre`(P|Div,Q), where Div is defined by

  ```
  agent Div = tau.Div.
  ```

- page 177, line -9: A better formulation is "naturaly when a valuation satisfies a given clock constraint or, alternatively ...".
  Thanks to Petr Jančar.

- page 183, Figure 10.3: The initial location Rest is bold instead of being denoted by a double circle like everywhere else in Part II of the book.
  Thanks to Roberto Gorrieri.

- page 189, Figure 10.4: Replace the action "hit!" with "hit".
  Thanks to Petr Jančar.

- page 189, Figure 10.4: The initial locations of the two timed automata are bold instead of being denoted by a double circle like everywhere else in Part II of the book.
  Thanks to Roberto Gorrieri.

- page 199, lines 5 and 9: Replace d' with d'', thrice per line.
  Thanks to Roberto Gorrieri.

- page 202, line 12: Remove ")" after 4.
  Thanks to Roberto Gorrieri.

- page 204, line -10: Replace "into eight classes" with "into five classes".
  Thanks to Petr Jančar.

- page 205, line -1: Swap "left" and "right".
  Thanks to Roberto Gorrieri.

- page 207, line 11 and 12: Change the formulation to "The number of equivalence classes of $\equiv$ still remains finite because we are finitely partitioning each equivalence class of an equivalence relation of finite index. (Recall that an equivalence relation has finite index

if it has only finitely many equivalence classes.)"
Thanks to Petr Jančar.

- page 207, first line of Equation (11.4): $v_y \leq c_y$ should read as $v(y) \leq c_y$.
Thanks to Roberto Gorrieri.

- page 209, line 9: Replace "... by a finite collection of clock constraints ..." with "... by a finite collection of extended clock constraints (see page 215 for the definition) ..."
Thanks to Petr Jančar.

- page 209, line -7: Replace "We can illustrate the automaton as follows:" with "We can picture the regions as follows:".
Thanks to Petr Jančar.

- page 210, line 6: Replace

$$[1 < x < 2, 1 < y < 2, x = y]_{\equiv}$$

with

$$[1 < x < 2, 0 < y < 1, \mathit{frac}(x) = \mathit{frac}(y)]_{\equiv} \ .$$

Thanks to Arnar Birgisson.

- page 212, line 7 and 9: Replace "iff" with "if". *Thanks to Petr Jančar.*

- page 213, line 1: Replace "the reflexive closure" with "the reflexive and transitive closure".
Thanks to Petr Jančar.

- page 213, line -9: The system "$T_u(A)$" should read as "$T_\epsilon(A)$ defined on page 198".
Thanks to Petr Jančar.

- page 214, line 14 (second line of Lemma 11.2): Replace "in A" with "in $T(A)$".
Thanks to Roberto Gorrieri.

- page 214, Lemma 11.2: This lemma does not hold as stated. The correct formulation is as follows.
Lemma 11.2 Let A be a timed automaton and (ℓ, v) a configuration. If $(\ell_0, v_0) \rightarrow^* (\ell, v)$ then $(\ell_0, [v_0]_{\equiv}) \Rightarrow^* (\ell, [v]_{\equiv})$. If $(\ell_0, [v_0]_{\equiv}) \Rightarrow^* (\ell, [v]_{\equiv})$ then for every $v_1 \in [v_0]_{\equiv}$ there is some $v' \in [v]_{\equiv}$ such that $(\ell_0, v_1) \rightarrow^* (\ell, v')$.
Proof: This lemma can be proven by induction on the length of the computation and the base case of the second claim follows from the statements made in Exercises 11.12, 11.13 and 11.14.
Thanks to Petr Jančar for noticing this.

- page 215, Exercise 11.23: Replace "the valuation v' defined by" with "the valuation v'' defined by". On the line below, "$v'(x)$" should read "$v''(x)$".
Thanks to Roberto Gorrieri.

- page 218, line -17: Change " ... for timed automata decidable in PSPACE ..." to " ... for deterministic timed automata decidable in PSPACE ...". The problem for nondeterministic automata is open but most likely not in PSPACE.

- page 233, line 16: Remove "$\mathcal{M}_t$" at the start of the line.
  Thanks to Roberto Gorrieri.

- page 233, lines -3 and -2: Replace "We wish to show that $(q', u + d') \models G$. Now, since p and q are timed bisimilar and $q \xrightarrow{d} d'$," with "We wish to show that $(q', u + d) \models G$. Now, since p and q are timed bisimilar and $q \xrightarrow{d} q'$,".
  Thanks to Arnar Birgisson and Unnar Thór Bachmann.

- page 236, line 12 (first line of Corollary 12.2): Remove "if,".
  Thanks to Roberto Gorrieri.

- page 243, lines -2 and -1: These should read as follows:

  (ℓ'', u'') of the timed automaton A,

  $$(\ell', u') \xrightarrow{a} (\ell'', u'') \text{ and } ((\ell'', u''), [y = 0]) \in S.$$

  Thanks to Unnar Thór Bachmann.

- page 244, lines 5–9: These should read as follows:

  Therefore, there exists a state (ℓ'', u'') of the timed automaton A such that

  $$(\ell', u') \xrightarrow{a} (\ell'', u'') \text{ and } (\ell'', u'') \text{ is timed bisimilar to } (\ell, [x = 0]) \ .$$

  Again by the definition of S, we may conclude that

  $$((\ell'', u''), [y = 0]) \in S,$$

  as required.

  Thanks to Unnar Thór Bachmann.

- page 252, line -16: "can be in location 2" should read "can be in location 1".
  Thanks to Unnar Thór Bachmann.

- page 253, line 8: "$i \in \{1, \ldots, n\}$." should read "$i \in \{0, \ldots, n\}$."
  Thanks to Arnar Birgisson.