Errata

Thanks to the Model Checking Reading Club at the Radboud University of Nijmegen, The Netherlandsw (in particular David N. Jansen and Frits W. Vaandrager), Dave Parker (Oxford University, UK), René Thiemann (U. Innsbruck, Austria), Ahmed Khademzadeh (Azad University of Mashhad, Iran), Alexander Nyßen and Daniel Weber (RWTH Aachen University) and the students at RWTH Aachen University attending the "Model Checking" lecture.

Comments are provided as:

⟨ page number ⟩ ⟨ line number ⟩ ⟨ short quote of the wrong word(s) ⟩ ▷ ⟨ correction ⟩

Chapter 1: System Verification

pp. 1, l. -5, *Pentium II* ▷ Pentium

pp. 5, l. 9, *lines of code lines* ▷ lines of code

pp. 5, l. footnote, *much higher* ▷ as the number of lines of code in the "golden" version of Windows95 is about 15 million, the error rate is in fact lower than normal.

pp. 6, l. 4, *Pentium II* ▷ Pentium

Chapter 2: Modeling Concurrent Systems

pp. 25, l. 11, *heading Example 2.8* ▷ Execution fragments of the Beverage Vending Machine

pp. 27, l. -15, *function* λ_y ▷ The function λ_y has no impact on the transitions (as suggested), but only affects the state labeling.

pp. 31, l. Fig. 2.3, *beer, soda* ▷ *bget* and *sget*, respectively

pp. 31, l. Fig. 2.3, *state with 1 beer, 2 soda* ▷ the grey circle should be a white circle.

pp. 46, l. Fig. 2.9, *locations in* PG_2 ▷ should be subscripted with 2 (rather than 1)

pp. 48, l. -1, $H = Act_1 \cap Act_2$ ▷ $H = (Act_1 \cap Act_2) \setminus \{ \tau \}$

pp. 51, l. Fig. 2.12, $T_1 \parallel T_2$ ▷ $TS_1 \parallel TS_2$ (this occurs twice)

pp. 51, l. -7, *all trains* ▷ the train

pp. 52, l. 3, *(above)* ▷ (page 54)

pp. 53, l. -1, *finite set of channels* ▷ set of channels

pp. 54, l. Fig. 2.16, *the transition labeled approach emanating from state* $\langle far, 3, down\rangle$ ▷ should be removed, and all the states that thus become unreachable

pp. 54, l. Fig. 2.16, *the transition labeled exit emanating from state* $\langle in, 1, up\rangle$ ▷ should be removed, and all the states that thus become unreachable

pp. 62, l. -3, *gen_msg(1)* ▷ *snd_msg(1)*

pp. 64, l. 4, *ack* ▷ message

pp. 65, l. Fig. 2.21, *second* **do** ▷ **od**

pp. 71, l. 15, *label in conclusion of inference rule* $c!e$ ▷ it is meant that the value of expression e is transferred; cf. Exercise 2.8, pp. 85

pp. 74, l. 1, $\xi[c := v_2 \dots v_k]$ ▷ $\xi' = \xi[c := v_2 \dots v_k]$

pp. 74, l. 1, $\xi[c := v_1 \dots v_k v]$ ▷ $\xi' = \xi[c := v_1 \dots v_k v]$

pp. 76, l. Figure 2.23 (top), x ▷ x'

Chapter 3: Linear-Time Properties

pp. 89, l. 9, *parallel systems* ▷ reactive systems

pp. 91, l. 7, *a deadlock occurs when all philosophers* ▷ a deadlock may occur when all philosophers

pp. 93, l. Fig. 3.3, *state* $available_i$ ▷ $available_{i,i}$

pp. 93, l. Fig. 3.3, *state* $available_{i+1}$ ▷ $available_{i,i+1}$

pp. 96, l. 3, *finite paths* ▷ finite path fragments

pp. 96, l. 4, *infinite path* ▷ infinite path fragment

pp. 101, l. -3, red_1 $green_2$ ▷ red_1, $green_2$

pp. 103, l. 11, $lwait_i$ ▷ $wait_i$

pp. 103, l. 11, $\exists k \geqslant j.\, wait_i \in A_k$ ▷ $\exists k \geqslant j.\, wait_i \notin A_k$

pp. 111, l. Theorem 3.21, $M = \sum_{s \in S} |Post(s)|$ ▷ $M = \sum_{s \in Reach(TS)} |Post(s)|$

pp. 111, l. 22, *The time needed to check* $s \models \Phi$ *is linear in the length of* Φ ▷ Add: This implicitly assumes that $a \in L(s)$ can be checked in $\mathcal{O}(1)$ time.

pp. 115, l. Lemma 3.27, *Proof* ▷ add the following sentence to the beginning of the proof: First note that for $P = (2^{AP})^\omega$ the claim trivially holds, since $\mathit{closure}(P) = P$ and the fact that P is a safety property since $\overline{P}$ is empty. In the remainder of the proof we consider $P \neq (2^{AP})^\omega$.

pp. 124, l. -3, *By definition* ▷ By Lemma 3.27

pp. 130, l. 3, *without being taken beyond* ▷ without being taken infinitely often beyond

pp. 131, l. 17, *assignment* $x = -1$ ▷ assignment $x := -1$

pp. 132, l. 2, *an execution fragment ... but not strongly A-fair.* ▷ an execution fragment that visits infinitely many states in which no A-action is enabled is weakly A-fair (as the premise of weak A-fairness does not hold) but may not be strongly A-fair.

pp. 134, l. 10, *any finite trace is fair by default* ▷ any finite trace is strongly or weakly fair by default

pp. 136, l. -5, *strong fairness property* ▷ fairness property

pp. 138, l. 4, *It forces synchronization actions to happen infinitely often.* ▷ It forces synchronization actions to happen infinitely often provided they are enabled infinitely often.

pp. 138, l. -14, *This requires that ... is enabled.* ▷ This requires that infinitely often a synchronization takes place when such synchronization is infinitely often enabled.

pp. 145, l. Exercise 3.5(g), *between zero and two* ▷ between zero and non-zero

Chapter 4: Regular Properties

pp. 157, l. -11, $w = A_1 \ldots A_n \in \Sigma$ ▷ $w = A_1 \ldots A_n \in \Sigma^*$

pp. 157, l. -10, *starts in* Q_0 ▷ starts in state Q_0

pp. 157, l. -4, Q_0 ▷ $\{ Q_0 \}$

pp. 158, l. -14, *NFAs can be much more efficient.* ▷ NFAs can be much smaller.

pp. 161, l. -9, *(2) ... for all* $1 \leqslant i < n$ ▷ ... for all $0 \leqslant i < n$. (Note: the invariant false has minimal bad prefix ε.)

pp. 161, l. -8, $1 \leqslant i < n$ ▷ $0 \leqslant i < n$

pp. 163, l. Example 4.15, *Minimal bad prefixes for this safety property constitute the language* $\{ \mathit{pay}^n \mathit{drink}^{n+1} \mid n \geqslant 0 \}$ ▷ Bad prefixes for this safety property constitute the language $\{ \sigma \in \left(2^{\{pay,drink\}}\right)^\omega \mid w(\sigma, \mathit{drink}) > w(\sigma, \mathit{pay}) \}$ where $w(\sigma, a)$ denotes the number of occurrences of a in σ.

pp. 164, l. -8, *path fragment* π ▷ initial path fragment π

pp. 164, l. -6, $TS \otimes \mathcal{A}$ *which has an initial state* $\triangleright$ $TS \otimes \mathcal{A}$ such that there exists an initial state

pp. 167, l. 7, 11, -4, $P_{inv(A)} \triangleright$ $P_{inv(\mathcal{A})}$

pp. 167, l. -2, $q_1, \ldots, q_n \notin F \triangleright$ Note: this condition is not necessary.

pp. 168, l. 1, $0 \leqslant i \leqslant n \triangleright$ $0 < i \leqslant n$

pp. 171, l. 8, *single word* $\triangleright$ a set contaning a single word

pp. 177, l. -7, *Example 4.13 on page 161* $\triangleright$ Example 4.14 on page 162

pp. 183, l. -3, -1, $\mathcal{L}_{q_1 q_3} = \ldots \triangleright$ $\mathcal{L}_{q_1 q_3} = C^*AB(B + BC^*AB)^*$

pp. 196, l. Example 4.57, *page 193* $\triangleright$ page 194

pp. 200, l. -7, $\bigwedge_{q \in Q} \triangleright$ $\bigwedge_{q \in F}$

pp. 206, l. Proof:, $TS = (S, Act, \rightarrow, I, AP) \triangleright$ $TS = (S, Act, \rightarrow, I, AP, L)$

Chapter 5: Linear Temporal Logic

pp. 230, l. 5, *eventually in the future* $\triangleright$ now or eventually in the future

pp. 236, l. Figure 5.2, $\triangleright$ It is assumed that $\sigma = A_0 A_1 A_2 \ldots$

pp. 276, l. -11, $\psi \in B$*if and only if* $\ldots \triangleright$ $\psi \in B$ if and only if $\ldots$

pp. 283, l. 10, $\neq \bigcirc \psi \in B$ *if and* $\ldots \triangleright$ $\neg \bigcirc \psi \in B$ if and $\ldots$

pp. 283, l. 17, *and* $\varphi = \bigcirc a \in B_1, B_2 \triangleright$ and $\varphi = a \in B_1, B_2$

pp. 287, l. -5, $|\neg(\mathit{fair} \rightarrow \varphi)| = |\mathit{fair}| + |\varphi| \triangleright$ $|\neg(\mathit{fair} \rightarrow \varphi)| = |\neg(\mathit{fair} \vee \neg\varphi)| = |\mathit{fair}| + |\varphi| + 3$

pp. 292, l. Figure 5.23, $\triangleright$ the self-loop at state $P(n)$ should be omitted

pp. 292, l. -1, $\bigcirc^{2i-1}(q, A, i) \rightarrow \triangleright$ *begin* $\wedge$ $\bigcirc^{2i-1}(q, A, i) \rightarrow$

pp. 294, l. -6, $\mathcal{G}_v arphi \triangleright$ $\mathcal{G}_\varphi$

pp. 303, l. Exercise 5.7(b), $\mathsf{W} \triangleright$ Y (to avoid confusion with unless)

Chapter 6: Computation Tree Logic

pp. 327, l. -12, *since* $\exists(\varphi \,\mathsf{U}\, \psi \vee \Box\varphi) \triangleright$ since $\forall(\varphi \,\mathsf{U}\, \psi \vee \Box\varphi)$

pp. 338, l. -5 and -6, $\triangleright$ transitions to s'_{n-1} are non-existing for n=0

pp. 342, l. -8 and -4, *maximal genuine* $\triangleright$ maximal proper

pp. 343, l. 4, *subformula of* Ψ $\triangleright$ subformula of Ψ'

pp. 345, l. -2, $Sat(\exists(\Phi \mathsf{U} \Psi)$ $\triangleright$ $Sat(\exists(\Phi \mathsf{U} \Psi))$

pp. 349, l. -9, $(a = c) \wedge (a \neq b)$ $\triangleright$ $(a \leftrightarrow c) \wedge (a \not\leftrightarrow b)$

pp. 351, l. Algorithm 15, $\triangleright$ comments in the first two lines of algorithm need to be swapped while replace E by T and TV by E

pp. 358, l. 11, $\triangleright$ Note that the length of $\Phi_n \in \mathcal{O}(n!)$

pp. 371, l. -6, *ifstatement* $\triangleright$ if statement

pp. 372, l. Algorithm 19, line 4, $C \cap Sat(b_j) \neq \varnothing$ $\triangleright$ $C \cap Sat(b_i) \neq \varnothing$

pp. 378, l. -6, *Eaxmple* $\triangleright$ Example

pp. 388, l. x, x'_1 $\triangleright$ pp.
, l. [, *1* $\triangleright$ e

x] 390Algorithm 20, line 4$f_{j+1}(\bar{x}) := f_{j+1}(\bar{x}) \vee \ldots f_{j+1}(\bar{x}) := f_j(\bar{x}) \vee \ldots$ pp. 391, l. Algorithm 21, line 4, $f_{j+1}(\bar{x}) := f_{j+1}(\bar{x}) \wedge \ldots$ $\triangleright$ $f_{j+1}(\bar{x}) := f_j(\bar{x}) \wedge \ldots$

pp. 393, l. Figure 6.21, right, *solid line* z_3 *between* 0 $\triangleright$ dashed line z_3 between 0

pp. 405, l. 2,3, $z = m = a_m, z_m = b_m, \ldots, z_i = a_i, z_i = b_i$ $\triangleright$ $z = m = a_m, y_m = b_m, \ldots, z_i = a_i, y_i = b_i$

pp. 469, l. Remark 7.19, line 10, $s_2 \models \varphi$, *but* $s_1 \not\models \varphi$ $\triangleright$ $s_2 \not\models \neg\varphi$, but $s_1 \models \neg\varphi$

Chapter 7: Equivalences and Abstraction

pp. 578, l. item 3., *self-loops* $[s]_{div} \to [s]_{div}$ $\triangleright$ self-loops $[s] \to [s]$

Chapter 10: Probabilistic Systems

pp. 778, l. 4, $\mathbf{P}'(s,t) = \ldots$ $\triangleright$

$$\mathbf{P}'(s,t) = \begin{cases} 1 & \text{if } s = t \text{ and } s \in B \cup S \setminus (C \cup B) \\ 0 & \text{if } s \neq t \text{ and } s \in B \cup S \setminus (C \cup B) \\ \mathbf{P}(s,t) & \text{otherwise.} \end{cases}$$

pp. 857, l. 2, $\sum_{s \in S_? \setminus \{s\}} \mathbf{P}(s,\alpha,t) \cdot x_t \triangleright - \sum_{s \in S_? \setminus \{s\}} \mathbf{P}(s,\alpha,t) \cdot x_t$

pp. 870, l. Lemma 10.119, *any* $s \in S \triangleright$ any $s \in T$

pp. 876, l. 11, $U_{\Box\Diamond P} \triangleright U_{\Box\Diamond B}$

pp. 903, l. Exercise 10.14, $\varphi = \Box \Diamond a \triangleright \varphi = \Diamond \Box a$

pp. 903/904, l. Exercise 10.17, *Markov chain* $\mathcal{M} \triangleright$ Markov chain $\mathcal{M}$ where all states are equally labeled

pp. 905, l. Exercise 10.22, $\triangleright$ Compute also the values $y_s = Pr^{\max}(s \models C \cup B)$ with $C = S \setminus \{ s_3 \}$ and $B = \{ s_6 \}$

pp. 905, l. Exercise 10.23, *(a), 1. and (b)* $\triangleright$ (a), (b), (c)

Appendix

pp. 918, l. 8, *not to 1* $\triangleright$ not to n