Errata to *Specifying Systems*

Leslie Lamport

17 February 2019

These are all the errors and omissions to the first printing (July 2002) of the book *Specifying Systems* reported as of 17 February 2019. Positions in the book are indicated by page and line number, where the top line of a page is number 1 and the bottom line is number −1. A running head and a page number are not considered to be lines, but all other lines are. Please report any additional errors to the author, whose email address is posted on `http://lamport.org`. The first person to report an error will be acknowledged in any revised edition.

Uncorrected Errors

page xiv

The table of contents should list the index, which begins on page 349. [First reported by Dominique Coutourier on 23 August 2002.]

page 36, line 3 and page 37, line 16

This is not an error, but it would be better if "tail" were replaced by "end". [First reported by Taj Khattra on 9 December 2004.]

page 32, line -11

Add the following footnote to that sentence.

> However, that section of the specification may not contain `(*` or `*)`, as in the string constant "`a*)b`".

[First reported by Damien Doligez on 27 February 2007.]

page 53

When the error on page 341, line 12 described below is corrected, a side note should be added beside the definition of *Tail* indicating that the actual definition of *Tail* in the *Sequences* module differs from the one given here. [First reported by Dominique Coutourier on 23 August 2002.]

page 54, line 21

Readers who want the function *Acker* to equal Ackermann's function should replace the last THEN expression $Acker[m-1,\ 0]$ with $Acker[m-1,\ 1]$. [First reported by Jesse Bingham on 16 March 2003.]

page 56, line 15

Replace "leave unchanged *vmem*" with "leave unchanged *wmem*". [First reported by Keith Marzullo on 1 October 2002.]

page 66, line 20

Add "page" before "341".
[First reported by Lásaro Jonas Camargos on 9 August 2004.]

page 71, lines 18–19

When the error on page 341, line 12 described below is corrected, the phrase "The definition of *Tail*" should be changed to "The definition of *Tail* given above". [First reported by Dominique Coutourier on 23 August 2002.]

page 89, line 4

Replace "pair of steps" by "pair of states". [First reported by Matthieu Lemerre on 28 October 2010.]

page 96, line −5

Replace $\langle Hnxt \rangle_{hr}$ by $\langle HCnxt \rangle_{hr}$.
[First reported by Santiago Zanella Béguelin on 11 June 2003.]

page 100, line 17

Replace "instead of (8.7)" by "instead of (8.6)". [First reported by Lucio Nardelli on 11 July 2010.]

page 115, lines −1 and −2

Replace "rdy" by "busy".
[First reported by Casey Klein on 15 February 2010.]

page 140, line -8

Replace $N(k)$ with N_k. [First reported by Rodrigo Schmidt on 9 November 2006.]

page 171, line -15

Before "and no submodules", add ", no assumptions,".
[First reported by Tom Rodeheffer on 3 October 2012.]

page 189, line -7

Add the missing space between "*opId*" and "to".
[First reported by Rodrigo Schmidt on 9 November 2006.]

page 234, line 8

Replace "on page 14.5.3" with "on page 261".
[First reported by William A. Welch on 25 July 2002.]

page 237, Section 14.2.5

The description of overriding should state that a Java class need not override all the definitions in a module. The definitions of operators not overridden are taken from the module. [First reported by Yuan Yu on 31 May 2002.]

page 243, line −13

Replace "*key*" with "*seed*". [First reported by Simon Zambrovski on 21 April 2009.]

page 252, line −13

Delete "*num*". [First reported by Jesse Bingham on 15 June 2004.]

page 256, footnote

Delete "though unlikely,". [First reported by Jesse Bingham on 15 June 2004.]

page 278, definition of *InfixOp*

The set of *InfixOp* token strings should include "`<=`" and "`\notin`". [First reported by Damien Doligez on 28 February 2007.]

page 278, definition of *InfixOp*

The set of *InfixOp* token strings should *not* include "`?`". [First reported by Damien Doligez on 6 December 2011.]

page 280ff

The BNF production for *G.Expression* is missing this alternative:

$$\mid G.Expression \ \& \ tok(\text{“.”}) \ \& \ Name$$

page 282, line 11

The production describing a tuple or finite sequence does not allow the empty sequence << >>. It should be replaced by

$$\mid \quad tok(\text{“<<”}) \ \&\ (Nil \mid CommaList(G.Expression)) \ \&\ tok(\text{“>>”}) \quad \langle 1,\, 2,\, 1+2 \rangle$$

[First reported by Chris Pacejo on 16 February 2019.]

page 289, line 15

This isn't an error, but the various possibilities would be better illustrated if this line were replaced by

$$\text{INSTANCE } M \text{ WITH } + \leftarrow Plus,\ Minus \leftarrow -$$

[First reported by Damien Doligez on 19 March 2007.]

page 293

The formula

$$\exists\, x, y \in S,\, z \in T \,:\, p \ \triangleq\ \exists\, x \in S \,:\, (\exists\, y \in S \,:\, (\exists\, z \in T \,:\, p))$$

is incorrect. It should state that the formulas on either side of the $\triangleq$ are equivalent if S and T contain no occurrences of x, y, or z. [First reported by Stephan Merz on 7 November 2006.]

page 303, bottom of page

To my surprise (and I think to his too), Stephan Merz discovered that the rules for the operator $[x \in S \mapsto e]$ are incomplete and the following additional rule should be added.

$$IsAFcn([x \in S \mapsto e])$$

[First reported by Stephan Merz on 2 August 2005.]

page 304, line 4

This "$\triangleq$" relation holds only for $n > 1$.

page 307, line -11

The list of characters that can appear in a string should include "!".
[First reported by Damien Doligez on 26 March 2007.]

page 316, line 11

The definition of $\sim_x$ should be

$$\sigma \sim_x \tau \triangleq \natural(\sigma_{x \leftarrow \{\}}) = \natural(\tau_{x \leftarrow \{\}})$$

where $\rho_{x \leftarrow \{\}}$ is the behavior obtained from a behavior ρ by replacing each of its states s with $s_{x \leftarrow \{\}}$. (We can replace $\{\}$ by any constant.) This makes obsolete the following erratum on the same line.
[First reported by Damien Doligez on 11 March 2016.]

page 316, line 11

The definition of $\sim_x$ should be

$$\sigma \sim_x \tau \triangleq \natural\sigma = [n \in \text{DOMAIN } \natural\tau \mapsto (\natural\tau[n])_{x \leftarrow \natural\sigma[n][\![x]\!]}]$$

[First reported by Raymond Boute on 5 October 2005.]

Section 17.4 (page 325ff)

The rules for defining the meaning of a λ expression do not prevent "variable capture" in all cases. A more sophisticated definition is needed. [First reported by Georges Gonthier on 9 May 2007.]

page 326, line -10

Between "e is" and "where", add "LET $Op \triangleq d$ IN exp".
[First reported by Rodrigo Schmidt on 9 November 2006.]

page 330-331, Section 17.5.5

This section fails to consider that the parameters p_i in the instantion (17.3) can appear in an instantiated theorem. Thus, the formula

$$\overline{A_1} \land \ldots \land \overline{A_k} \Rightarrow \overline{T}$$

can contain the p_i as undeclared parameters. If all the p_i are ordinary parameters, then the instantiated theorem added to *Thm* can be written as:

$$\forall\, p_1, \ldots, p_m \,:\, \overline{A_1} \land \ldots \land \overline{A_k} \Rightarrow \overline{T}$$

However, if some of the p_i are operator parameters, then the instantiated theorem cannot be represented in the version of TLA$^+$ described in the book. It can be written in the current version of TLA$^+$ as:

$$\begin{array}{ll} \text{ASSUME} & \text{NEW } p_1, \ldots, \text{NEW } p_m \\ \text{PROVE} & \overline{A_1} \land \ldots \land \overline{A_k} \Rightarrow \overline{T} \end{array}$$

[First reported by Tom Rodeheffer on 5 October 2012.]

page 331, line 16

Change k to n.
[First reported by Tom Rodeheffer on 5 October 2012.]

page 332, Section 17.5.6

The two forms

$$\text{THEOREM } Op \triangleq exp \qquad \text{and} \qquad \text{ASSUME } Op \triangleq exp$$

were not part of the language as of the publication of the book, so all reference to them should have been omitted. However, these forms have been added to the current version of the language (sometimes called TLA^{+2}).
[First reported by Rodrigo Schmidt on 9 November 2006.]

pages 337–338

The two bulleted subitems of item 2 at the bottom of page 337 should be modified so that, before doing the indicated substitutions in A, B, and C, the following substitutions are performed to their subexpressions, for any e and v:

$$\begin{array}{ll} \text{UNCHANGED } v & \rightarrow\ v' = v \\ [e]_v & \rightarrow\ e \lor (v' = v) \\ \langle e \rangle_v & \rightarrow\ e \land (v' \neq v) \end{array}$$

[First reported by Yuan Yu on 1 October 2002.]

page 341, line 12

The definition of *Tail* in the *Sequences* module defines the tail of the empty sequence to be the empty sequence. The tail of the empty sequence should be left unspecified. One possible definition is:

$$\begin{array}{lll} Tail(s) & \triangleq & \text{IF } Len(s) \neq 0 \text{ THEN } [i \in 1 \,..\, (Len(s) - 1) \mapsto s[i+1]] \\ & & \text{ELSE CHOOSE } n : \text{FALSE} \end{array}$$

page 344, lines 14ff

The explanation of % and $\div$ should add the condition that $a \div b$ is an integer.
[First reported by Tom Rodeheffer on 10 July 2013.]

page 345, module *Peano*

The definition of *PeanoAxioms* needs the following additional conjunct asserting that the function Sc is injective.

$$\land\ \forall\, m, n \in N : (Sc[m] = Sc[n]) \Rightarrow (m = n)$$

[First reported by Stephan Merz on 3 August 2005.]

page 347, line 17

In this comment, "continuity condition" should be changed to "monotonicity condition". [First reported by Peter Hancock on 13 August 2002.]

Index

The index should contain the entries

octal representation, 308
numbers, representation of, 308

The entry for "string" should also include a reference to page 47.