The theory and practice of concurrency: Errata

Version of May 21, 1999

My apologies for the following errors and any others there may be. Do let me know if you find any others so that they can be added to this list and corrected in any re-prints.

Since the errors in a few of the exercises in Part II may inconvenience people teaching from this part, I have put a revised version of the affected exercises (plus, perhaps, a few clarifications to others not mentioned below) on the web site for you to download.

Chapter 1

Page 18 Insert 'more than' before 'one' on line -3 (i.e., third from bottom).

Page 20 In line 2 of paragraph 4, replace *Card* by *CARD*.

Page 25 Insert full stop between 'CSP' and 'However' on line 8.

Page 25 Reverse $>$ in *ABS* definitions (i.e., replace it by $<$ so that the definitions do compute a non-negative absolute value rather than the non-positive value given by the printed definitions).

Page 27 (Line -4) Insert 'is' between 'This' and 'the $\{\mid c_1, c_2 \mid\}$ notation'.

Page 33 In line 4 of paragraph after 1.21, insert 'over' between 'as well as' and '$\sqcap$'.

Page 40 Delete 'its' between UFP; and 'theoretical' on line 6 of 4th paragraph.

Chapter 2

Page 54 In the last line of the middle display (i.e., last line of the Example) replace P by q, so it now reads

$$\sqcap\ (\mathit{refuse} \rightarrow (\mathit{out.card} \rightarrow q) \sqcap \mathit{STOP})))$$

Page 64 Lines 2 and 3: replace x by y inside the set of amounts accepted on channel *dispense*: $\{y \in \mathit{WA} \mid y \geq M\}$, and replace $\mathit{CUSTspend}_M$ by $\mathit{CUSTspend}_x$.

Chapter 3

Page 83 Last non-footnote line: insert ? after opining bracket on RHS of equation.

Page 85 In the last displayed line, $B_2^1(y)$ should be replaced by $B_1^2(y)$.

Chapter 4

Page 108 $\Box$ is missing before the third line of the definition of *Succ*.

Chapter 5

Page 115 Remove extra 's' from 'over-optimisstic' on line 2.

Page 119 Spurious 'a' after $\sqcap$ in line 7.

Chapter 7

Pages 168/169 The reference which begins at the bottom of page 168 should be to Figure 2.3 on page 60.

Chapter 8

Exercise 8.2.4 (page 191) Replace quicksort by $\mathit{Zero}_{/\!/}$. (The present version is too subtle for an initial example of this type of analysis. There is an extensive discussion of the different forms of constructiveness exhibited by *Qsort* and $\mathit{Zero}_{/\!/}$ in the solutions to exercises.)

Page 199 Definition of $\mathit{failures}_\perp(P \setminus X)$: first X on second line should be Y:

$$\begin{array}{rcl} \mathit{failures}_\perp(P \setminus X) & = & \{(s \setminus X, Y) \mid (s, Y \cup X) \in \mathit{failures}_\perp(P)\} \\ & & \cup\, \{(s, Y) \mid s \in \mathit{divergences}(P \setminus X)\} \end{array}$$

Exercise 8.3.8 (page 207) Insert comma after 'page 197'.

Exercise 8.4.2 (page 214) 'singe' should be 'single'

Chapter 9

Page 228 Insert full stop after [94,97] on line 8.

Exercise 9.3.2 (page 238) Reword part (a) to

> Show that axioms F2, F4 and a much weakened F3 (dealing only with two cases that can occur in connection with ✓) suffice to create a model whose members are exactly the failure-sets that arise in $\mathcal{F}$. *We no longer get the full version of F3 because it relates refusal sets to successor traces, and by leaving out the trace component it thus becomes impossible to include this particular 'sanity check'.*

Page 237 The construction of $CFD_{(s,X)}[V]$ given here is insufficiently subtle because it cannot (under the test $\mathbf{T}_3$) distinguish between a process which can refuse a set and one which cannot but diverges immediately afterwards. In the former case the test is failed (as intended) by immediate deadlock; in the latter it is failed because the construction hides the event which is accepted leading to the divergence.

The result stated in Theorem 9.3.1 (iii) is correct, but $CFD_{(s,X)}[V]$ needs modification to prove it. The trick is to hide the events leading up to the prospective refusal but not the events testing the refusal itself. This can be achieved by modifying the definitions of $W(n)$ and $CFD_{(s,X)}[V]$ to the following:

$$CFD_{(s,X)}[V] \;=\; ((C_{(s,X)}[V][\![a, b/x, x \mid x \in \Sigma]\!]) \underset{\{a,b\}}{\|} W(\#s)) \setminus \{a\}$$

where

$$\begin{aligned} W(0) &= b \to CS \\ W(n) &= (a \to W(n-1)) \,\Box\, CS \quad (n > 0) \\ CS &= c \to CS \end{aligned}$$

and a, b, c are arbitrary members of Σ.

This works because only the first $\#s$ events (necessarily those corresponding to V performing the trace s) are hidden. If an event from X is accepted, this will result in a non-hidden b so that, even if V diverges immediately after this event, it will not create an *immediate* divergence of the process $CFD_{(s,X)}[V]$. Note how we have succeeded in selectively hiding the first $\#s$ events by using a double renaming construction which maps each event to two others. There are similarities with the double renamings used on pages 401 and 454.

I am grateful to Antti Valmari who pointed out both the flaw and the fix.

Chapter 11

Exercise 11.1.1 (page 271) There are not enough laws here for the stated purpose (since the two zero laws are both right-zeros). You can recover my intended solution either by replacing one of them by the corresponding left zero law, for example

$$\perp \parallel P = \perp$$

or by adding in the symmetry law for $\parallel$ that can be found in Exercise 11.4.5. My suggested amendment for the purpose of setting the exercise is to replace law (1) by the above.

Neither of these in itself achieves my stated aim of giving three disjoint sets of laws from Hinchey and Jarvis that prove all processes equal (in the first case because the book concerned only contains the right zero laws). This can, in fact, be done properly (from the pure equality laws in their book) in various ways. It can be done retaining as two of them the sets of of laws in Exercises 11.4.5 and 11.5.3, but the third set (at least in my approach) is rather too long to be elegant. It is nicer to change both of the sets in 11.1.1 and 11.4.5 so that they become, respectively

$$\begin{array}{rcl} P \parallel \perp & = & \perp \\ P \parallel \mathit{STOP} & = & \mathit{STOP} \\ P \parallel Q & = & Q \parallel P \\ \perp \bigtriangleup Q & = & \perp \\ \mathit{STOP} \bigtriangleup Q & = & Q \end{array}$$

and

$$\begin{array}{rcll} P \,\Box\, \mathit{RUN} & = & P & \\ P \,\Box\, \mathit{STOP} & = & P & \\ P \,\Box\, Q & = & Q \,\Box\, P & \\ P \mid\mid\mid \mathit{STOP} & = & P & \\ P \mid\mid\mid \mathit{RUN} & = & \mathit{RUN} & \Leftrightarrow \mathit{divergences}(P) = \{\} \end{array}$$

I would be interested to hear if anyone can extend the number of disjoint sets of laws (for proving all or most processes equal) from the offending text beyond 3. You should only use their conventional 'equality' laws, it being too easy if their mysterious 'inequality' laws are permitted thanks to the logical truth that from $\phi \wedge \neg\phi$ you can infer anything. The problem in taking the number beyond 3 is not any lack of false laws (one that looks promising and I have not used is $P \mid\mid\mid P = P$) but rather the fact that one uses up the true ones in completing the different proofs that all processes are equal.

Page 275 $\setminus \{\mid \mathit{left} \mid\}$ is missing three times in the displayed formula in middle of the page.

Chapter 12

Page 295 'thana' should be substituted by 'than' (line 3).

Exercise 12.2.1 (page 308) remove definition of L' (which is unused); substitute $L \setminus X$ in last line of p308 by $H \setminus X$.

Exercise 12.2.2 (page 309) Additionally assume S only communicates in L; for clarity replace all '$\Sigma \setminus L$'s by H; the subscript P in the last displayed formula should be H.

Exercise 12.4.1 (page 325) In part (c), the second displayed line should have the additional clause $Y \cap L = \{\}$.

Chapter 13

Page 339 Line -8 inster 'on' between 'agreeing' and 'at least.

Page 341 Insert subscript i on the only P without a subscript in the first definition on this page.

Page 349 There is a missing end of definition marker after the definition of cyclic communication networks.

Chapter 14

Page 387 Insert 'but' between 'this' and 'that' at the end of the first line after the display in the middle of the page.

Page 390 The definition of *SpeedReg(j)* needs an extra line so that it allows time to pass when there is no train in the segment:

$$\begin{array}{rcl} \mathit{SpeedReg}(j) & = & \mathit{enter}?t!j \rightarrow \mathit{SpeedReg}'(j,0) \\ & & \mathit{tock} \rightarrow \mathit{SpeedReg}(j) \end{array}$$

Page 413 'conpcurrency' becomes 'concurrency' (line 5 of Notes)

Chapter 15

Page 443 In the last display (the definition of `Memory`), replace `f(v)` by `f(a)`.

Page 461 Replace '$pk(A)$' by '$pk(B)$' as the subscript in the final line ($\beta.3$, left-hand version) of the attack. (The right-hand version of this is printed correctly.)

Appendix A

Page 490 Line 4 of paragraph 3: replace ϵ by δ.

Appendix B

Page 498 Insert `not` before right-hand side of the third equivalence at the top of this page.

Page 511 The process in the middle of the page equivalent to the indexed sequential choice should read

```
c.1.2->c.1.3->c.2.1->c.2.3->c.3.1->c.3.2->SKIP
```

Page 511 The set `{1..n}` in the last displayed process should be replaced with the sequence `<1..n>` as the replicated version of `[a <-> b]` is always indexed by a sequence, not a set.

Bibliography

Page 546 citation [65] Replace 'TACAS '97' by 'TACAS '96'.

Page 547 citation [79] There is a spurious comma after 'Olderog'.

Index

Page 555 There are separate entries for 'fixed point induction' and 'fixed-point induction'. Obviously these should be combined.