Errata, CS_411: Critical Systems, Lent Term 2002

Anton Setzer

May 9, 2002

A0: Introduction

- p. 22. Replace “Apparently nobody looked for a bug in the software” by “The architecture of the software was investigated but no detailed search for a bug was done”.

- p. 27. Replace “written examination in January” by “written examination in May”.


Further the plan has been adapted:
B2 is now called “Data types”. B3 is “Propositions as types”. B4 is “Interactive programs in dependent type theory. B5 is “Case studies”.

A1: Safety criteria

- p. 1: Replace (d) “Identification of System Requirements” by “Identification of Safety Requirements”.

- p. 11: Insert in second bullet bewteen “by which the” and “of equipment or plant” the word “safety”.

- p. 12: Insert between (vii) and (viii) a new idem (vii) “Security”. Dependability gets new number (ix).

- p. 15: Replace in first bullet 9998/1000 by 9998/10000.

A2: Hazard analysis

- p. 9, first bullet: Replace “FMFA” by “FMEA”.

*Dept. of Computer Science, University of Wales Swansea, Singleton Park, Swansea SA2 8PP, UK. Email: a.g.setzer@swan.ac.uk
B1: Introduction

- Replace everywhere in this section in formulas type by Type.
- p. 5: Replace “Alf, a graphical user interface for Agda” by “Alfa, a graphical user interface for Agda, but Alfa can be used to create Agda code”.
- p. 13: Insert after “will allow us to carry out the following steps:” the following: “Assume \( f :: A \to B \) and \( a :: A \) have been introduced.”
- p. 17: Replace the conclusion of the first elimination rule “\( \pi_0(a) : A \)” by “\( \pi_0(c) : A \)”.
- p. 19: Add in the last item after “For instance” “(assuming \( A :: Type, a, b :: A \))”:
- p. 20: Replace in the last paragraph “substitute” by “substituting” and “remaining” by “renaming”.
- p. 21: Replace “\( (x :: B) \to ? :: A \)” by “\( (x :: B) \to ? :: B \to A \)”.
- p. 29: Replace in the premisse of the rule “\( \Rightarrow \)” by “\( \to \)”.
- p. 35: In the Introduction rule, add the additional first premisse \( x :: A \Rightarrow B :: Type \).
  Further add this premisse in the equality rules and omit the comment “(The last two rules assume \( x :: A \Rightarrow B :: Type \)).”
- p. 51: In the rules presented after “In fact when solving the above . . .”, replace in the conclusion \( B \) by \( A \to B \).
  In the last formula, replace \( \lambda(a :: A) \to \{ ! ! \} :: B \) by \( \lambda(a :: A) \to \{ ! ! \} :: A \to B \).
- p. 59: In the last rule, replace in the conclusion the type \( B \) by \( B[x := a] \).

B2: Data types

- p. 0. Replace “Change for Plan of Stream B1” by “Change for Plan of Stream B”.
- p. 8. Insert “in” in line 4 after “Choose while the cursor”.
- p. 9. Interchange \( \text{true@} \), and \( \text{false@} \) in the definition of \( f \).
- p. 21. The type of \( \text{inr} \) is \( \text{inr} : (A, B : \text{Set}) \to B \to A + B \).
  Further in the type of \( \text{Plus} \_\text{Split} \), the type of \( C \) should be \( A + B \to \text{Set} \) and the type of \( \text{sr} \) should be \( (b : B) \to C \) (\( \text{inr} A B b \)).
- p. 22: The type of \( \text{inr}(\text{A+B}) \) is \( B \to (A+B) \).
  Further insert in the following item between “This can be” and “using the menu “agda-infer-type” the word “checked”.
- p. 29: The type of \( B \) in the type of \( \text{Sigma} \) should be \( A \to \text{Set} \).
• p. 45: S∅N isn’t recognized by Alfa. An extra slide B2-45a explaining this has been inserted.

• p. 46: Replace twice

\[
f \ (n : : \ N) \\
\rightarrow \ A
\]

by

\[
f \ (n : : \ N) \\
:: \ A
\]

• p. 49: In the defining equation of (+) (first formula, at the end };} has to be replaced by {;].

• p. 50: In the defining equation of (+) (first formula, at the end {;}] has to be replaced by {;].

• p. 51, 52 are essentially correct (except see below), but have been rewritten using some improved notation. What was not correct:
  - In the definition of prod, “(B : : \ N)” should be replaced by “(B : : Set”.
  - In the last line “(Vec A n)” has to be replaced by “(Vec A m’)”.
  - On page 52, (A:: NVec n) has to be replaced by avec, (B:: NVec n) has to be replaced by bvec.

• Between p. 51 and 52, some additional explanations were added.

• p. 54: In the first case distinction on m, replace (S n’) by (S m’). (This was not a mistake, but the improvement makes it easier to understand this).

• p. 67, add before (a_{in} :: A_{in}) an arrow \to.

**Labsession2**

• p. 1, second bullet (●): Omit “(ie. true or false)”.

• p. 2, second bullet (●): replace “Agda” by “alfa”.

• p. 2, last bullet (●): replace “dvipso” by “dvips”.

**Labsession2**

• p. 2, third bullet (●): Replace in the last line of the definition of sym “:: Eqnat n k” by “:: Eqnat m n”.

3