Formalised Inductive Reasoning in the Logic of Bunched Implications : Errata

James Brotherston

Dept. of Computing, Imperial College London

This document describes an error in the original version of the paper, and how it has been corrected in the new version of the paper, which is available from the author's webpage.

In the original version of the paper, the induction rule for an inductive predicate P_j is formulated on page 10 using the following schema, writing H_k for the induction hypothesis associated with the predicate P_k:

$$\dfrac{\text{minor premises} \qquad \Gamma(\Delta; H_j\mathbf{t}) \vdash F}{\Gamma(\Delta; P_j\mathbf{t}) \vdash F}\;(\text{Ind } P_j)$$

where there is a minor premise for each production featuring in its conclusion an inductive predicate P_i that is mutually dependent with P_j:

$$\dfrac{C(\mathbf{x})}{P_i\mathbf{t}(\mathbf{x})} \qquad \Longrightarrow \qquad \Delta; C_H(\mathbf{x}) \vdash H_i\mathbf{t}(\mathbf{x}) \quad (\forall x \in \mathbf{x}.\, x \notin FV(\Delta))$$

(See the paper for relevant definitions.)

However, this formulation is unsound in general, as can be seen by considering the following $\mathrm{LBI_{ID}}$ proof of the invalid sequent $I \to \bot; \mathtt{ls}\, t\, u \vdash u = 0$:

$$\dfrac{\dfrac{\dfrac{}{I \vdash I}\,(\text{Id}) \quad \dfrac{\dfrac{}{\bot \vdash x = 0}\,(\bot\text{L})}{\bot; I \vdash x = 0}\,(\text{Weak})}{I \to \bot; I \vdash x = 0}\,(\to\text{L}) \quad \dfrac{\dfrac{\dfrac{}{I \to \bot; (x \mapsto x', \top) \vdash 0 = 0}\,(=\text{R})}{I \to \bot; (x \mapsto x', y = 0) \vdash y = 0}\,(=\text{L})}{I \to \bot; x \mapsto x' * y = 0 \vdash y = 0}\,(*\text{L}) \quad \dfrac{\dfrac{}{u = 0 \vdash u = 0}\,(\text{Id})}{I \to \bot; u = 0 \vdash u = 0}\,(\text{Weak})}{I \to \bot; \mathtt{ls}\, t\, u \vdash u = 0}\,(\text{Ind } \mathtt{ls})$$

where `ls` is the "linked list segment" predicate whose definition is given in Example 2.7 in the paper and whose induction rule is given in Example 3.5, and the application of (Ind `ls`) employs the induction variables z_1, z_2 and the induction hypothesis $z_2 = 0$.

That the formulation of the induction rule is unsound is due to the presence of the assumptions Δ in the minor premises. In the situation of first-order logic, the minor premises define a prefixed point of the monotone operator for the inductive predicates (cf. Defn 2.4 in the paper) and, because the variables used in the minor premises are chosen fresh, this can be demonstrated in full generality even in the presence of extra assumptions drawn from the left of the conclusion sequent. However, in the setting of BI, the same argument fails because though the variables in the minor premises are chosen fresh, the resource state is not, and that the minor premises define a fixed point of the monotone operator is not established in full generality because in order to do so we must make an assumption about the resource state, namely that it satisfies Δ.

By dropping Δ from the minor premises, as is done in the corrected version of the paper, soundness is restored; note e.g. that we are no longer able to prove the first minor premise in the example above. (Note also that dropping Δ from the minor premises means that explicit mentions of Δ can also be dropped from the conclusion and major premise.) This change percolates through to the example induction rules given in Examples 3.4 and 3.5, but not to any of the other definitions or results in the paper. A typo is also corrected: the variables $\mathbf{x}$ used in the minor premises should be fresh with respect to Γ rather than Δ.