Errata of my PhD thesis “Superposition for Higher-Order Logic”

Alexander Bentkamp

Selection of positive literals

The calculi in Chapter 6 and 7 allow selection of positive literals if they are of the form $t \approx \bot$. The completeness theorems does not hold up when using this feature.

Here is where the proof breaks: In case 1.2 of the proof of Lemma 6.21, the conclusion of the indicated superposition inference is not necessarily smaller than the main premise C. For example, rewritten subterm of C might be at the topmost position of the left-hand side of a non-maximal, selected positive literal $u \approx \bot$ in C, and D might contain a literal $u \approx u''$ such that $u' \succ u'' \succ \bot$.

Moreover, case 5 in the proof of Lemma 6.22 does not work. $R_N^*|_{\prec C} \not\models s \approx \bot$ only implies that s is not reducible to $\bot$, but does not imply that s is reducible to $\top$. Also, even if s is reducible to $\top$ by $R_N^*|_{\prec C}$, it does not necessarily follow that it is reducible by R_C.

In short, selection of literals of the form $t \approx \bot$ should not be allowed in Definition 6.2 and 7.17.

Minor Errata

Page 91 The sentence “Neither s nor $\lambda w.\, \mathsf{g}\,(y\,w)$ are fluid.” should say “Neither s nor $\lambda w.\, \mathsf{g}\,(\mathsf{db}^1\; w)$ are fluid.”

Page 182 The sentence “We must show that C is true in $\mathcal{I}$ under ξ.” should say “We must show that C is true in $\mathcal{I}'$ under ξ.”

Page 127 The proof of Lemma 6.8 is wrong. The term $s\{x \mapsto u\}$ is not necessarily structural smaller than t so induction hypothesis does not apply. The proof can be fixed as follows:

Lemma 6.8 *Under the requirements of Definition 6.6, we have* $[\![t]\!]_R = [t]$ *for all* $t \in \mathcal{T}_{\mathrm{G}}$.

Proof. By well-founded induction on t using the left-to-right lexicographic order on $(n(t), |t|)$, where $n(t)$ is the number of quantifiers in t and $|t|$ is the size of the term t.

If $t = \mathsf{f}(\bar{s})$, then $[\![t]\!]_R = \mathcal{J}(\mathsf{f})([\![\bar{s}]\!]_R) \overset{\text{IH}}{=} \mathcal{J}(\mathsf{f})([\bar{s}]) = [\mathsf{f}(\bar{s})] = [t]$. The application of the induction hypothesis is justified because for all i, $(n(t), |t|) > (n(s_i), |s_i|)$.

If $t = \forall x.\ s$, then we proceed as follows: Let $\mathcal{T}_{\mathrm{QFG}} \subseteq \mathcal{T}_G$ be the set of quantifier-free ground terms. We observe that for all ground terms $u \in \mathcal{T}_G$, there exists a quantifier-free ground term $u' \in \mathcal{T}_{\mathrm{QFG}}$ such that $u \leftrightarrow_R^* u'$. This follows from (I1) because any quantifier term is of Boolean type. Therefore, we have

$$\min\{[\![s]\!]_R^{\{x\mapsto[u]\}} \mid u \in \mathcal{T}_{\mathrm{G}}\} = \min\{[\![s]\!]_R^{\{x\mapsto[u]\}} \mid u \in \mathcal{T}_{\mathrm{QFG}}\}$$

and

$$\min\{[s\{x \mapsto u\}] \mid u \in \mathcal{T}_{\mathrm{G}}\} = \min\{[s\{x \mapsto u\}] \mid u \in \mathcal{T}_{\mathrm{QFG}}\}$$

It follows that

$$\begin{aligned}
[\![t]\!]_R &= \min\{[\![s]\!]_R^{\{x\mapsto[u]\}} \mid u \in \mathcal{T}_G\} && \text{by the definition of term denotation}\\
&= \min\{[\![s]\!]_R^{\{x\mapsto[u]\}} \mid u \in \mathcal{T}_{\mathrm{QFG}}\} && \text{by the observation above}\\
&= \min\{[\![s\{x \mapsto u\}]\!]_R \mid u \in \mathcal{T}_{\mathrm{QFG}}\} && \text{by Lemma 6.7}\\
&= \min\{[s\{x \mapsto u\}] \mid u \in \mathcal{T}_{\mathrm{QFG}}\} && \text{by the induction hypothesis}\\
&= \min\{[s\{x \mapsto u\}] \mid u \in \mathcal{T}_G\} && \text{by the observation above}\\
&= [\forall x.\ s] && \text{by (I4)}\\
&= [t]
\end{aligned}$$

The application of the induction hypothesis is justified because $s\{x \mapsto u\}$ contains less quantifiers than t.

If $t = \exists x.\ s$, we argue analogously. $\square$

Page 128 The proof of (I1) in part (5) of Lemma 6.10 is incomplete because (I1) requires us to show that $\top \not\leftrightarrow_{R^*}^* \bot$.

Here is why $\top \not\leftrightarrow_{R^*}^* \bot$: For a proof by contradiction, suppose that $\top \leftrightarrow_{R^*}^* \bot$. Since R^* is confluent and $\top$ is in normal form, we have $\bot \rightarrow_{R^*}^* \top$. By the assumption that the heads of the left-hand sides of rules in R are not logical symbols, we know that there is no rule of the form $\bot \rightarrow t$ in R. By (B1) no rules in Δ_R^s have the form $\bot \rightarrow t$. Thus, R^* does not contain rules of the form $\bot \rightarrow t$, a contradiction.

Page 131 The definition of an inference *reducing* a counterexample should be as follows: An inference *reduces* a counterexample C if its main premise is C, its side premises are true in R_N^*, and its conclusion D is a clause smaller than C and false in R_N^*. In particular, the conclusion D is not required to be in N, contrary to what the the original formulation suggested.

Page 133 Case 2.4 of the proof of Lemma 6.21 can be simplified: We do not need to inspect the reduction chain of $s \approx t$. By (I3), $s \approx t \rightarrow_{R_N^*}^* \bot$ implies directly that $R_N^* \not\models s \approx t$.

Acknowledgments I would like to thank Yicheng Qian for discovering many of these errata and for suggesting fixes for many of them.