Note on admissibility of a higher order frame rule in regional logic

David A. Naumann
Stevens Institute of Tech., Hoboken, NJ, USA
naumann@cs.stevens.edu

This is a note concerning a draft paper entitled “Regional logic for local reasoning about global invariants” (RL for short), by Banerjee, Rosenberg, and myself, July 2007. The paper includes a “higher order frame rule” inspired by that of separation logic. The rule is shown to be sound under strong conditions, which amount to conditions on the derivation of one of the antecedents—an abomination, or at least tasteless and of questionable value.

The purpose of this note is to show that this unpleasantry is easily avoided. I describe a straightforward reformulation of the proof system, supporting an ordinary interpretation of the rule as imposing conditions on antecedents, not on proofs of antecedents. (Contrary to the comment in section 7 of RL, I do not need to introduce new program syntax like the expose blocks of Spec#.) The rule was originally not presented as definitive in any sense, but rather illustrative of the regional logic, and this note is in the same spirit.

The hypothetical frame rule in RL is presented as an ordinary rule for correctness judgements. But then a notion of “robust decomposition” is defined for proof trees, and RL shows that the hypothetical frame rule is sound—in fact admissible—provided that it’s antecedent correctness judgement is derived by a proof with a robust decomposition.

Informally, a robust decomposition of a proof tree is a collection of designated subtrees in which there are no procedure calls—let me call this the inner reasoning,1 which involves the small axioms and fine grained effects—and in which certain rules are not used outside the designated subtrees—call that the outer reasoning. Moreover, a condition is imposed on the root of each designated subtree; that condition pertains to the “commitment” and “client effect” used in the hypothetical frame rule.

What I do here is to distinguish two different judgement forms, and thereby force every derivation to correspond to one in RL with a robust decomposition.

The new proof system uses the subsidiary judgements (independence, frames, etc) unchanged from RL. For correctness rules, we use the following:

inner rules: Rules for judgements of the form

\[ \vdash \{ \theta \} C \{ \theta' \} \{ \varepsilon \} \]

These are retained in their original form, not as hypothetical judgements with partitioned effect set (as in section 6). We retain all the rules from section 5 of RL.

outer rules: Rules for hypothetical judgements of the form

\[ \Delta \vdash_{\gamma, \pi_B} \{ \theta \} C \{ \theta' \} \{ \pi_C; \pi_M \} \]

The difference from RL is that now the turnstyle is subscripted with a commitment \( \gamma \) and a top-level effect \( \pi_B \). These are propagated unchanged through the rules for this judgement, and are not otherwise mentioned in those rules, with two exceptions (rule InnerToOuter and HypFrame discussed later).

The rules for this judgement are like what was described in RL section 6—except that we do not include hypothetical versions of the small axioms and we do not include effect elimination. Specifically: There are hypothetical versions of

- the structural rules of fig 9—but not the effect-elimination rules of fig 10;
- the control structure rules Seq, If, While, and Var of fig 8—but not the axioms Alloc, Assign, FieldAcc, FieldUpd, Assign Pos, FieldUpd Pos.
- Procedure invocation, i.e., rule ProcIntro in section 6 of RL.

inner to outer: inner judgements are promoted by rule

\[ \text{InnerToOuter} \]

\[ \vdash \{ \varphi \} C \{ \varphi' \} \{ \varepsilon \} \quad \varphi' \Rightarrow \gamma \quad \gamma \vdash \varepsilon \leq \pi_B \]

\[ \vdash_{\gamma, \pi_B} \{ \varphi \} C \{ \varphi' \} \{ \varepsilon \} \]

1 I was tempted to refer to the “local” and “global” parts of the reasoning, but this risks confusion, so I chose inner/outer for lack of something better.
hypothesical frame rule: This is as in RL except for propagating the commitment and client effect by requiring them in the antecedent.

\[
\text{Hyp Frame} \quad \begin{align*}
Q; \overline{x} \text{ frames } \psi & \quad \overline{x} \neq \overline{B} \\
\text{regions}(\overline{B}) = R_1, \ldots, R_n & \quad \gamma \Rightarrow Q \# R_1 \cup \ldots \cup R_n \\
\{ \delta \} k \{ \delta' \} [\overline{x}_k] \vdash \gamma, \overline{x}_B \{ \varphi \} & \quad C \{ \varphi' \}[\overline{C}; \overline{M}] \\
\{ \delta \wedge \psi \} k \{ \delta' \wedge \psi \} [\overline{x}_k] \vdash \{ \varphi \wedge \psi \} B \{ \varphi' \wedge \psi \}[\overline{B}; \overline{M}]
\end{align*}
\]

I refrain from decorating the turnstyle of the conclusion of Hyp Frame since the aim here is not a comprehensive proof system but an illustrative one. Let’s say Hyp Frame derives a third kind of correctness judgement, of a main program with respect to its library code.

It is routine to check that a proof in my system maps directly to a proof together with a robust decomposition in the logic of PL. **Caveat:** I omitted the restriction that the Subst rule is not used for variables in \( \overline{x} \). That can be enforced by decorating the judgements the way I did for the commitment and client effect; I omitted that just for brevity.

Now we can argue that Hyp Frame is admissible, in the new logic, following the lines of the old proof. We conjoin \( \psi \) throughout the outer judgements. For reasons given in RL, this yields correct rule instances in every case except at the instance of InnerToOuter where \( \psi \) is added in the conclusion but missing from the antecedent. This we can fix by inserting an instance of Frame before InnerToOuter; this changes the implication required by InnerToOuter to be \( \varphi' \wedge \psi \Rightarrow \gamma \) which of course holds since \( \varphi' \Rightarrow \gamma \) in the original proof.