Working Paper Series
ISSN 1177-777X

CONSIDERING REACHABILITY WHEN COMPARING DATA REFINEMENTS

Steve Reeves

Working Paper: 12/2008
November 2008

Department of Computer Science
The University of Waikato
Private Bag 3105
Hamilton, New Zealand

Considering reachability when comparing data refinements

Steve Reeves

Department of Computer Science, University of Waikato, Hamilton, New Zealand
November 3, 2008 10:44

Abstract. Adding considerations about reachability to the *Logics of Specification Languages* [1] chapter [2].

1 Reachability concerns

We need to think about *reachability*. It seems to me that the counterexample given in the chapter [2] relies exactly on having a simulation that is not well-defined, in the sense that it does not "deal" with all reachable states (made clearer soon!).

An ADT may never be able to reach some of its states because there is no sequence of operations, starting with the initialisation, which allows us to pass to those states. This also means we have to think of all the operations in an ADT, including the initialisation and finalisation operations, since reachability is a property of the whole ADT, not of single operations within an ADT. So, we'll assume that an ADT A is given by $< S_A, \{O_i^A\}_i, I_A, F_A >$ where S_A are the states that the ADT may be in, the O_i^A are the operations of the ADT, and I_A and F_A are its initialisation and finalisation operations respectively. (And note that, as is usual in these sorts of presentation, we use $\star$ to name the state from the global state space S_G which the ADT is called from and returns control to after it has done its work.)

Now consider the three "shapes" of diagrams which have to semi-commute, i.e. the initialisation and finalisation ones, and the operation ones. These give rise to the usual conditions, for conformal ADTs A and C and simulation S,

$$
\begin{array}{l}
I_C \subseteq I_A \fatsemi S \\
S \fatsemi O_i^C \subseteq O_i^A \fatsemi S \\
S \fatsemi F_C \subseteq F_A
\end{array}
$$

For these to hold there are certain readings to do with reachability.

From the third case, if $(t_C, \star) \in F_C$ then there must be a t_A such that $(t_A, \star) \in F_A$ and $(t_A, t_C) \in S$. So, if t_C is reachable then $\exists\, t \in S_A \bullet (t, t_C) \in S$.

Other conditions on simulations can be read off these conditions, but we need just one rule (below) for our purposes in the current enterprise, and the reading here is enough to give us that. The conditions when read together mean that a simulation must be defined everywhere on $reach(A)$ and onto $reach(C)$, i.e. $reach(A) \subseteq \mathrm{dom}\, S$ and $reach(C) \subseteq \mathrm{ran}\, S$.

Definition 1. *For ADT A (taken from [3], p. 80—and see the surrounding discussion there for consideration of reachability))*

$$reach(A) =_{def} \bigcap \{S \subseteq S_A \mid I_A(S_G) \subseteq S \wedge \forall\, O_i^A \bullet O_i^A(S) \subseteq S\}$$

where $O^A(X)$ are the states reachable from a state in $X \subseteq S_A$ by (one) use of operation O^A, i.e.

$$O^A(X) =_{def} \{s \in X \mid \exists\, t \bullet (t, s) \in O^A\}$$

We then need to add conditions to what counts as a simulation in order to enforce the property that simulations are well-defined in terms of reachability.

So, we have:

Definition 2. *A simulation $S \subseteq T_1 \times T_0$ is acceptable with respect to ADT C if*

$$\forall\, t_0 \in T_{0\perp} \bullet t_0 \in reach(C) \Rightarrow \exists\, t_1 \in T_{1\perp} \bullet t_1 \star t_0' \in \vec{S}$$

This definition gives us a new rule that we use in the proof of equivalence (denoted by ♠ there) later:

Lemma 1. *With the usual conditions on y we have:*

$$\frac{t_0 \in reach(C) \quad y \star t_0' \in \vec{S} \vdash P}{P}$$

2 Strict lifting

Definition 3 (Strictly Lifted Forward Simulation).

$$S^{\mathbb{P}(\vec{T_1} \curlyvee T_0')} =_{df} \{z_1 \star z_0' \in T_{1_\perp} \star T_{0_\perp}' \mid (z_1 \neq \perp \Rightarrow z_1 \star z_0' \in S) \wedge (z_1 = \perp \Rightarrow z_0' = \perp')\}$$

Various introduction and elimination rules follow from this.

Lemma 2. *The following additional rules are derivable for strictly-lifted simulations:*

$$\frac{}{S \subseteq \vec{S}}\ (i) \qquad \frac{}{\vec{S} \subseteq \vec{S}}\ (ii) \qquad \frac{}{\perp \in \vec{S}}\ (iii)$$

$$\frac{t_1 \star \perp' \in \vec{S}}{t_1 = \perp}\ (iv) \qquad \frac{t_1 \star t_0' \in \vec{S} \quad t_0' \neq \perp'}{t_1 \star t_0' \in S}\ (v)$$

□

Lemmas 2($iv - v$) embody the strictness captured by definition 3: if the after state is $\perp$ then the initial state must also be $\perp$, and if it is not $\perp$ then the initial state was not either. **WF$_\ominus$-Refinement** is a refinement theory, in which both the operations and the simulation are strictly lifted. WF$_\ominus$-refinement was defined in the chapter [2] as follows:

Definition 4.

$$U_0 \overset{s}{\sqsupseteq}_{wf_\ominus} U_1 =_{df} \vec{S} \fatsemi \overset{\ominus}{U_0} \subseteq \overset{\ominus}{U_1} \fatsemi \vec{S}$$

Various introduction and elimination rules follow from this definition.

Lemma 3. *Let z_0 and z_1 be fresh.*

$$\frac{z_1 \star z_0' \in \vec{S} \fatsemi \overset{\ominus}{U_0} \vdash z_1 \star z_0' \in \overset{\ominus}{U_1} \fatsemi \vec{S}}{U_0 \overset{s}{\sqsupseteq}_{wf_\ominus} U_1} (\sqsupseteq^+_{wf_\ominus}) \qquad \frac{U_0 \overset{s}{\sqsupseteq}_{wf_\ominus} U_1 \quad t_1 \star t_0' \in \vec{S} \fatsemi \overset{\ominus}{U_0}}{t_1 \star t_0' \in \overset{\ominus}{U_1} \fatsemi \vec{S}} (\sqsupseteq^-_{wf_\ominus})$$

□

We also then need to condition the definition of the refinement relation to consider just those states that are reachable (unreachable ones clearly play no rôle). The following definition incorporates reachability into Definition 4 above.

Definition 5. *For operations U_0 and U_1 from conformal ADTs C (with states T_0) and A (with states T_1) respectively, and for acceptable simulation S we have:*

$$U_0 \overset{s}{\sqsupseteq}_{wf_\ominus} U_1 =_{df} \forall\, t_0 \in T_{0\perp} \bullet t_0 \in reach(C) \Rightarrow \forall\, t_1 \in T_{1\perp} \bullet (t_1 \star t_0' \in \vec{S} \fatsemi \overset{\ominus}{U_0} \Rightarrow t_1 \star t_0' \in \overset{\ominus}{U_1} \fatsemi \vec{S})$$

This definition gives rise to just the original rules in Lemma 3 with the addition that everything is conditioned on the assumption that we are dealing with reachable states. In the proofs that follow we will tend not to record this assumption or its use in order to simplify the presentation since it becomes crucial in only one place right at the end of our final proof. So, until that point (which is clearly flagged) we will use the unconditioned rules for simplicity.

We begin by showing that $\text{WF}_\ominus$-refinement implies SF-refinement by proving that $\text{WF}_\ominus$-refinement satisfies both SF-refinement elimination rules. Firstly the rule for preconditions.

Proposition 1. *The following rule is derivable:*

$$\frac{U_0 \overset{s}{\sqsupseteq}_{wf_\ominus} U_1 \quad Pre\ U_1\ t_1 \quad t_1 \star t_0' \in S}{Pre\ U_0\ t_0}$$

Proof.

$$\dfrac{\dfrac{\delta}{\vdots}\ t_1 \star \perp' \in \overset{\ominus}{U_1} \fatsemi \vec{S} \qquad \dfrac{\dfrac{\dfrac{}{t_1 \star y' \in \overset{\ominus}{U_1}}(2) \quad \dfrac{\dfrac{}{y \star \perp' \in \vec{S}}(2)}{y = \perp}(L.\ 2(iv))}{t_1 \star \perp' \in \overset{\ominus}{U_1}}(=) \qquad Pre\ U_1\ t_1}{t_1 \star \perp' \in U_1}(\ominus_0^-)}{false}(L.\ 4)}{Pre\ U_0\ t_0}(2, U_\fatsemi^-)\ (1, \neg^+, \neg^-)$$

where δ is:

$$\dfrac{U_0 \overset{s}{\sqsupseteq}_{wf_\ominus} U_1 \qquad \dfrac{\dfrac{t_1 \star t_0' \in S}{t_1 \star t_0' \in \vec{S}}\ (L.\ 2(i)) \qquad \dfrac{\dfrac{\dfrac{t_1 \star t_0' \in S}{t_0 \in T_0}}{t_0 \in T_{0_\perp}}\ (L.\ 5(iv)) \qquad \dfrac{\overline{\neg Pre\ U_0\ t_0}\ (1)}{t_0 \star \perp' \in \overset{\ominus}{U_0}}}{t_1 \star \perp' \in \vec{S} \fatsemi \overset{\ominus}{U_0}}\ (U^+_\fatsemi)}{t_1 \star \perp' \in \overset{\ominus}{U_1} \fatsemi \vec{S}}\ (\sqsupseteq^-_{wf_\ominus})$$

□

Turning now to the second elimination rule in SF-refinement.

Proposition 2. *The following rule is derivable:*

$$\dfrac{U_0 \overset{s}{\sqsupseteq}_{wf_\ominus} U_1 \quad Pre\ U_1\ t_1 \quad t_0 \star t_2' \in U_0 \quad t_1 \star t_0' \in S \quad t_1 \star y' \in U_1, y \star t_2' \in S \vdash P}{P}$$

where the usual conditions apply to the eigenvariable y.

Proof.

$$\dfrac{\dfrac{U_0 \overset{s}{\sqsupseteq}_{wf_\ominus} U_1 \qquad \dfrac{\dfrac{t_1 \star t_0' \in S}{t_1 \star t_0' \in \vec{S}}\ (L.\ 2(i)) \qquad \dfrac{t_0 \star t_2' \in U_0}{t_0 \star t_2' \in \overset{\ominus}{U_0}}\ (L.\ 5(i))}{t_1 \star t_2' \in \vec{S} \fatsemi \overset{\ominus}{U_0}}\ (U^+_\fatsemi)}{t_1 \star t_2' \in \overset{\ominus}{U_1} \fatsemi \vec{S}}\ (\sqsupseteq^-_{wf_\ominus}) \qquad \begin{array}{c}\delta\\ \vdots \\ P\end{array}}{P}\ (1, U^-_\fatsemi)$$

where δ is:

$$\dfrac{\dfrac{\dfrac{\overline{}\ (1)}{t_1 \star y' \in \overset{\ominus}{U_1}} \qquad Pre\ U_1\ t_1}{t_1 \star y' \in U_1}\ (\ominus^-_0) \qquad \dfrac{\overline{}\ (1)}{y \star t_2' \in \vec{S}} \qquad \dfrac{\dfrac{\overline{}\ (1)}{t_1 \star y' \in \overset{\ominus}{U_1}} \qquad Pre\ U_1\ t_1}{\dfrac{t_1 \star y' \in U_1}{y \neq \perp}\ (L.\ 4)}\ (\ominus^-_0)}{y \star t_2' \in S}\ (L.2(v))}{t_1 \star y' \in U_1 \wedge y \star t_2' \in S}\ (\wedge^+)$$
$$\vdots$$
$$P$$

□

Theorem 1.

$$U_0 \sqsupseteq_{wf_\ominus} U_1 \Rightarrow U_0 \sqsupseteq_{sf} U_1$$

Proof. This follows immediately, by $(\sqsupseteq^{+}_{sf})$, from propositions 1 and 2. □

We now show that SF-refinement satisfies the $\mathrm{WF}_{\ominus}$-elimination rule.

Proposition 3. *The following rule is derivable:*

$$\frac{U_0 \sqsupseteq_{sf} U_1 \quad t_1 \star t'_0 \in \vec{S} \mathbin{\fatsemi} \overset{\ominus}{U_0}}{t_1 \star t'_0 \in \overset{\ominus}{U_1} \mathbin{\fatsemi} \vec{S}}$$

Proof.

$$\dfrac{\dfrac{}{Pre\ U_1\ t_1 \vee \neg\ Pre\ U_1\ t_1}\ (LEM) \qquad \begin{matrix}\delta_0, \delta_1 \\ \vdots \\ t_1 \star t'_0 \in \overset{\ominus}{U_1} \mathbin{\fatsemi} \vec{S}\end{matrix}}{t_1 \star t'_0 \in \vec{S} \mathbin{\fatsemi} \overset{\ominus}{U_0} \qquad t_1 \star t'_0 \in \overset{\ominus}{U_1} \mathbin{\fatsemi} \vec{S}}\ (2, \vee^{-})}{t_1 \star t'_0 \in \overset{\ominus}{U_1} \mathbin{\fatsemi} \vec{S}}\ (1, U^{-}_{\fatsemi})$$

where δ_0 is:

$$\dfrac{U_0 \sqsupseteq_{sf} U_1 \quad \dfrac{}{Pre\ U_1\ t_1}\ (2) \quad \begin{matrix}\beta_0 \\ \vdots \\ y \star t'_0 \in U_0\end{matrix} \quad \dfrac{\dfrac{}{t_1 \star y' \in \vec{S}}\ (1) \quad \dfrac{\dfrac{}{Pre\ U_1\ t_1}\ (2)}{t_1 \neq \bot}\ (L.4)}{t_1 \star y' \in S}\ (L.2(v)) \quad \begin{matrix}\beta_1 \\ \vdots \\ \end{matrix}}{t_1 \star t'_0 \in \overset{\ominus}{U_1} \mathbin{\fatsemi} \vec{S}}\ (3, \sqsupseteq^{-}_{sf_1})$$

where β_0 stands for the following branch:

$$\dfrac{\dfrac{}{y \star t'_0 \in \overset{\ominus}{U_0}}\ (1) \quad \dfrac{U_0 \sqsupseteq_{sf} U_1 \quad \dfrac{}{Pre\ U_1\ t_1}\ (2) \quad \dfrac{\dfrac{}{t_1 \star y' \in \vec{S}}\ (1) \quad \dfrac{\dfrac{}{Pre\ U_1\ t_1}\ (2)}{t_1 \neq \bot}\ (L.4)}{t_1 \star y' \in S}\ (L.2(v))}{Pre\ U_0\ y}\ (\sqsupseteq^{-}_{sf_0})}{y \star t'_0 \in U_0}\ (\ominus^{-}_{0})$$

and β_1 is:

$$\dfrac{\dfrac{\dfrac{}{t_1 \star w' \in U_1}\ (3)}{t_1 \star w' \in \overset{\ominus}{U_1}}\ (L.5(i)) \quad \dfrac{\dfrac{}{w \star t'_0 \in S}\ (3)}{w \star t'_0 \in \vec{S}}\ (L.2(i))}{t_1 \star t'_0 \in \overset{\ominus}{U_1} \mathbin{\fatsemi} \vec{S}}\ (U^{+}_{\fatsemi})$$

δ_1 stands for the following branch:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{t_1 \star y' \in \vec{S}}\ (1)}{t_1 \in T_{1\bot}}}{t_1 = \bot \vee\ t_1 \in T_1} \qquad \begin{matrix}\epsilon_0, \epsilon_1 \\ \vdots \\ t_1 \star t'_0 \in \overset{\ominus}{U_1} \mathbin{\fatsemi} \vec{S}\end{matrix}}{t_1 \star t'_0 \in \overset{\ominus}{U_1} \mathbin{\fatsemi} \vec{S}}\ (*, \vee^{-})$$

ϵ_0 stands for the following branch:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{t_1 = \bot}\,(*) \quad \dfrac{}{t_1 \star y' \in \vec{S}}\,(1)}{y = \bot} \quad \dfrac{}{y \star t_0' \in \overset{\ominus}{U_0}}\,(1)}{t_0 = \bot} \quad \dfrac{}{\bot \star \bot' \in \overset{\ominus}{U_1} \underset{9}{\circ} \vec{S}}}{\bot \star t_0' \in \overset{\ominus}{U_1} \underset{9}{\circ} \vec{S}}\,(=) \quad \dfrac{}{t_1 = \bot}\,(*)}{t_1 \star t_0' \in \overset{\ominus}{U_1} \underset{9}{\circ} \vec{S}}\,(=)$$

ϵ_1 stands for the following branch:

$$\dfrac{\dfrac{\dfrac{}{t_1 \in T_1}\,(*) \quad \dfrac{}{\neg\, Pre\ U_1\ t_1}\,(3) \quad \dfrac{\dfrac{}{x \star t_0' \in \vec{S}}\,(4)}{x \in T_{1_\bot}}}{t_1 \star x' \in \overset{\ominus}{U_1}}\,(L.5(v)) \quad \dfrac{}{x \star t_0' \in \vec{S}}\,(4)}{t_1 \star t_0' \in \overset{\ominus}{U_1} \underset{9}{\circ} \vec{S}}\,(U_{\underset{9}{\circ}}^{+}) \qquad (\spadesuit, 4)$$

$$t_1 \star t_0' \in \overset{\ominus}{U_1} \underset{9}{\circ} \vec{S}$$

□

To get the above step at ♠ to work we need the reachability definitons etc.. Note that this is where the proof before failed, so considering reachability, which we failed to do in the original paper, has allowed us to show that the two refinements *are* equivalent.

Theorem 2.

$$U_0 \sqsupseteq_{sf} U_1 \Rightarrow U_0 \overset{s}{\sqsupseteq}_{wf_\ominus} U_1$$

□

Theorems 1 and 2 together establish that the theories of SF-refinement and $WF_\ominus$-refinement are equivalent.

Theorem 3.

$$U_0 \sqsupseteq_{wf_\ominus} U_1 \iff U_0 \sqsupseteq_{sf} U_1$$

□

Comments: I daresay much of this can be used to extend equivalence results for the other cases. I had hoped that we'd be able to ditch the LEM requirement, but it seems not!

3 Some machinery

Natural carriers for each type (sets which exclude $\bot$) are then easily defined by closing:

$$\Upsilon =_{df} \{z^{\Upsilon} \mid z \neq \bot\}$$

under the type forming operations. When we are working in this more general framework, we sometimes need the following:

Lemma 4.

$$\frac{\bot \in U}{false} \qquad \frac{Pre\ U\ t}{t \neq \bot}$$

Lemma 5.

$$\frac{}{U \subseteq \overset{\ominus}{U}}\ (i) \qquad \frac{}{\overset{\ominus}{U} \subseteq \overset{\bullet}{U}}\ (ii) \qquad \frac{}{\bot \in \overset{\ominus}{U}}\ (iii)$$

$$\frac{\neg\ Pre\ U\ t \quad t \in T^{in}_{\bot}}{t \star \bot' \in \overset{\ominus}{U}}\ (iv) \qquad \frac{\neg Pre\ U\ t_0 \quad t_0 \in T^{in} \quad t'_1 \in T^{out'}_{\bot}}{t_0 \star t'_1 \in \overset{\ominus}{U}}\ (v)$$

Notice that in (v) t_0 ranges over the natural carrier set, rather than the extended carrier.
□

Corollary 1.

$$\frac{t' \in T^{out'}_{\bot}}{\bot \star t' \in \overset{\bullet}{U}}\ (i) \qquad \frac{\neg\ Pre\ U\ t \quad t \in T^{in}_{\bot}}{t \star \bot' \in \overset{\bullet}{U}}\ (ii)$$

□

References

1. Bjørner, D., Henson, M., eds.: Logics of Specification Languages. EATCS. Springer (2008)
2. Henson, M.C., Deutsch, M., Reeves, S.: Z logic and its applications. In: Logics of Specification Languages. EATCS. Springer (2008) 489–596
3. de Roever, W.P., Engelhardt, K.: Data Refinement: Model oriented proof methods and their comparison. Number 47 in Cambridge Tracts in Theoretical Computer Science. Cambridge University Press (1998)