Relational Updates in Views

Adam Wright

August 30, 2012

This document assumes you are familiar with the notation of the Views paper. Specifically, you need to recall that:

1. A View is a commutative semigroup $(\textsc{Views}, *)$, where p, q, r range over $\textsc{Views}$.
2. There are machine states, $\textsc{States}$
3. There is a reification funciton $\lfloor : \rfloor \, \textsc{States} \to \mathcal{P}(\textsc{Views})$.
4. There is semantic entailment relation $\preccurlyeq \subset \textsc{Views} \times \textsc{Views}$
5. There are a set of machine actions $\textsc{Actions}$, ranged over by α which includes at least the identity action $\textsc{id}$. These actions are state transformers on machine states, $\alpha : \textsc{States} \to \mathcal{P}(\textsc{States})$. The transformer for $\textsc{id}$ is $\textsc{id}(\mathbf{s}) = \{\mathbf{s}\}$.

Definition 1 (Semantic Consequence Rule)**.**

$$\frac{p \preccurlyeq p' \quad \{\ p'\ \}\ \mathbb{C}\ \{\ q'\ \} \quad q' \preccurlyeq q}{\{\ p\ \}\ \mathbb{C}\ \{\ q\ \}}$$

Definition 2 (Generalised Frame Rule)**.**

$$\frac{\{\ p\ \}\ \mathbb{C}\ \{\ q\ \}}{\{\ f(p)\ \}\ \mathbb{C}\ \{\ f(q)\ \}}$$

The soundness of these rules relies on the following properties of $\preccurlyeq$ and f.

Definition 3 (Requirements of semantic consequence relations)**.** A choice of relation $\preccurlyeq$ is sound if it preserves all frames:

$$\forall p, q \in \textsc{Views}.\ p \preccurlyeq q \implies \forall r \in \textsc{Views}.\ \lfloor p * r \rfloor \subseteq \lfloor q * r \rfloor$$

Definition 4 (Requirements of generalised frame functions)**.** A choice of function f is sound if is preserves all actions under frames:

$$\forall p, q \in \textsc{Views}, \alpha \in \textsc{Actions}. \quad \begin{array}{c} (\forall r \in \textsc{Views}.\ [\![\alpha]\!]\ \lfloor p * r \rfloor \subseteq \lfloor q * r \rfloor) \\ \implies \\ (\forall r \in \textsc{Views}.\ [\![\alpha]\!]\ \lfloor f(p) * r \rfloor \subseteq \lfloor f(q) * r \rfloor) \end{array}$$

We can generalise the Generalised Frame Rule further. Consider taking f as a relation, R. The Generalised Frame Rule then renders as:

Definition 5 (Relational Frame Rule)**.**

$$\frac{p'\ R\ p \quad \{\ p'\ \}\ \mathbb{C}\ \{\ q'\ \} \quad q'\ R\ q}{\{\ p\ \}\ \mathbb{C}\ \{\ q\ \}}$$

Note that if R is functional, then this rule collapses to the Generalised Frame Rule.
The soundness of this rule relies on the following properties of R :

Definition 6 (Requirements of relational frame relations)**.** A choice of relation R is sound if it is both left-total:

$$\text{For all } p \in \textsc{Views}, \text{ there exists some } q \in \textsc{Views} \text{ such that } p \ R \ q$$

and if it preserves all actions under frames:

$$\forall p, q \in \textsc{Views}, \alpha \in \textsc{Actions}. \quad \begin{array}{c} (\forall r \in \textsc{Views}.\ [\![\alpha]\!]\ \lfloor p * r \rfloor \subseteq \lfloor q * r \rfloor) \\ \Longrightarrow \\ (\forall r, p', q' \in \textsc{Views}.\ p \ R \ p' \wedge q \ R \ q' \implies [\![\alpha]\!]\ \lfloor p' * r \rfloor \subseteq \lfloor q' * r \rfloor) \end{array}$$

The first is the natural extension of the generalised frame rule requirement. The second (left totality) is sufficient to ensure cases such as $\{\ p'\ \} \ \mathbb{C} \ \{\ q'\ \}$ where $p' \ R \ p$ but there is no q such that $q' \ R \ q$ are not permitted. Were such relations allowed, the proof obligation to check actions would become vacuous, and we could pick a relation showing the divergence of any code.

Lemma 1 (The Relational Frame rule is sound)**.** *Let R be a relation satisfying the properties in definition 6. Then, derivations using the View inference rules and the relational frame rule using R are sound.*

Proof. This is proven as another case of the general views soundness result. The proof is basically identical to the frame rule case, where we know that that $\alpha| \ \vdash \{p_r\}\{p'_r\}$ by the left totality and action preservation properties. □

It is interesting to examine choices of relation in which *both* the rule of sementic consequence and the relational frame rule are applicable. Examining the rules, it is clear the only difference between generalised frame and semantic consequence is the order of the precondition relationship, and the stronger proof requirements. Consider then, relations $\mathcal{R}$ which are symmetric and reflexive.

Lemma 2 (Frame/Consequence freedom)**.** *Let $\mathcal{R} \subset \textsc{Views} \times \textsc{Views}$ be a symmetric, reflexive relation. Then, $\mathcal{R}$ satisfies the requirements of a sementic consequence relation if and only if it satisfies the requirements of a relational frame relation.*

Proof. **Right direction** $\rightarrow$: We first show that if $\mathcal{R}$ is a semantic consequence relation, it is a relational frame relation. We thus have the following properties by assumption:

1. $\mathcal{R}$ is symmetric.
2. $\mathcal{R}$ is reflexive.
3. $\forall p, q \in \textsc{Views}.\ p \ \mathcal{R} \ q \implies \forall r \in \textsc{Views}.\ \lfloor p * r \rfloor \subseteq \lfloor q * r \rfloor$

We must show the conditions of definition 6. Left totality is straightforward (all reflexive relations are left total). For the action preservation property, consider properties 1 and 3. Together, these imply that if $p \ \mathcal{R} \ q$, then $\forall r \in \textsc{Views}.\ \lfloor p * r \rfloor = \lfloor q * r \rfloor$. The requirement for action preservation then follow directly from the premise of the implication we are required to show.

Left direction $\leftarrow$: We now show that if $\mathcal{R}$ is a relational frame relation, it is a semantic consequence relation. We thus have the following properties by assumption:

1. $\mathcal{R}$ is symmetric.
2. $\mathcal{R}$ is reflexive.
3. $\mathcal{R}$ is left-total.
4. $$\forall p, q \in \textsc{Views}, \alpha \in \textsc{Actions}. \quad \begin{array}{c} (\forall r \in \textsc{Views}.\ [\![\alpha]\!]\ \lfloor p * r \rfloor \subseteq \lfloor q * r \rfloor) \\ \Longrightarrow \\ (\forall r, p', q' \in \textsc{Views}.\ p \ \mathcal{R} \ p' \wedge q \ \mathcal{R} \ q' \implies [\![\alpha]\!]\ \lfloor p' * r \rfloor \subseteq \lfloor q' * r \rfloor) \end{array}$$

We must show it satisfies the conditions of definition 3. In assumption 4, pick $\alpha = \text{ID}$, $p = q$. Expanding, we derive:

$$(\forall r \in \text{VIEWS}.\ \lfloor p * r \rfloor \subseteq \lfloor p * r \rfloor)$$
$$\Longrightarrow$$
$$(\forall r, p', q' \in \text{VIEWS}.\ p\ \mathcal{R}\ p' \wedge q\ \mathcal{R}\ q' \implies \lfloor p' * r \rfloor \subseteq \lfloor q' * r \rfloor)$$

which is equivalent to

$$(\forall r, p', q' \in \text{VIEWS}.\ p\ \mathcal{R}\ p' \wedge q\ \mathcal{R}\ q' \implies \lfloor p' * r \rfloor \subseteq \lfloor q' * r \rfloor)$$

Now pick $p' = p$ and $q' = q$. Expanding, we derive

$$(\forall r \in \text{VIEWS}.\ p\ \mathcal{R}\ p \wedge p\ \mathcal{R}\ q \implies \lfloor p * r \rfloor \subseteq \lfloor q * r \rfloor)$$

The first conjunction is discharged by assumption 2 (reflexivity). Ergo:

$$p\ \mathcal{R}\ q \implies \forall r \in \text{VIEWS}.\ \lfloor p * r \rfloor \subseteq \lfloor q * r \rfloor$$

which was to be shown. □

0.1 Conclusions

In some sense, both the generalised frame rule and semantic consequence rules are methods of joining proofs together. The frame rule takes a more general proof, and specialises it, when that specialisation has no effect on the validity of the original proof. We can thus join the generalist proof to more specific cases - the very essence of modular reasoning. The semantic consequence rule increases the number of times one can reuse a proof, by revealing that the state represented in a derivation is actually sufficient (from a proof validity perspective) connect to the other proof.

The results herein show that, for certain types of proof transformation that one might call "ghost state updates", it makes no formal difference whether one presents the updates as some kind of semantic consequence or frame rule.