Automatic Computation of Static Variable Permissions

John C. Reynolds
Carnegie Mellon University

MFPS, May 28, 2011

Research partially supported by National Science Foundation Grant
CCF-0916808

Introduction

We will describe a procedure for inferring permissions for the proof system described by Uday S. Reddy in “Syntactic Control of Interference for Concurrent Separation Logic” (presented earlier at this conference).

Given a purported proof in Reddy’s formalism in which the variable permissions have been erased, our goal is to determine if there is an assignment of permissions that will give a valid proof.

Contexts

Reddy uses contexts such as

$$\overbrace{x^{p^x}, y^{p^y}, z^{p^z}}^{\Sigma} \mid \overbrace{r_1(x^{p^{1x}}, y^{p^{1y}})\colon R_1, r_2(x^{p^{2x}}, z^{p^{2z}})\colon R_2}^{\Gamma} \vdash \cdots$$

(We assume that the contexts are in normal form.) We introduce the set

$$\text{Owners} = \text{Resources} \cup \{\mathbf{self}\},$$

and treat Σ as a list associated with $\mathbf{self}$. We also break out the resource invariants as a separate part of the context:

$$\mathbf{self}(x^{p^x}, y^{p^y}, z^{p^z}), r_1(x^{p^{1x}}, y^{p^{1y}}), r_2(x^{p^{2x}}, z^{p^{2z}}) \mid \overbrace{r_1\colon R_1, r_2\colon R_2}^{\Upsilon} \vdash \cdots$$

Then we transpose the (Owner, Variable)-matrix to bring the variables to the outside:

$$\overbrace{x(\mathbf{self}^{p^x}, r_1^{p^{1x}}, r_2^{p^{2x}}), y(\mathbf{self}^{p^y}, r_1^{p^{1y}}), z(\mathbf{self}^{p^z}, r_2^{p^{2z}})}^{\Delta} \mid \overbrace{r_1\colon R_1, r_2\colon R_2}^{\Upsilon} \vdash \cdots$$

Contexts (continued)

We limit our development to fractional permissions, which are real numbers in the set

$$\text{Perms} = \{\, p \mid 0 < p \leq 1 \,\}.$$

However, rather than regarding a context Δ as a partial function into permissions, we will extend it to a total function by filling in the missing permissions with the nonpermission 0. Thus a permission context is a function

$$\Delta\colon \text{Vars} \to \text{Owners} \to \text{Perms} \cup \{0\},$$

such that

$$\textstyle\sum_{o \in \text{Owners}} \Delta\, v\, o \leq 1.$$

We assume that Vars and Owners are finite sets.

Judgements

The judgements used by Reddy:

$$\Sigma \vdash E\ \mathbf{Exp} \quad \Sigma \vdash P\ \mathbf{Assert}$$

$$\Sigma \vdash x\ \mathbf{Var} \quad \Sigma|\Gamma \vdash \{P\}\ C\ \{Q\}.$$

become, with our altered view of contexts:

$$\Delta|\Upsilon \vdash E\ \mathbf{Exp} \quad \Delta|\Upsilon \vdash P\ \mathbf{Assert} \qquad \text{(passive)}$$

$$\Delta|\Upsilon \vdash x\ \mathbf{Var} \quad \Delta|\Upsilon \vdash \{P\}\ C\ \{Q\}. \qquad \text{(active)}$$

To deal with the Rule of Consequence, we will also need a passive judgement that an assertion is valid:

$$\Delta|\Upsilon \vdash P\ \mathbf{Valid}. \qquad \text{(passive)}$$

Passive judgements are those which only describe the reading of variables, while *active* judgements may describe writing as well. (Our presentation is simplified by using the same form of context for all judgements.)

A *pre-judgement* has the form

$$\Upsilon \vdash E\ \mathbf{Exp} \quad \Upsilon \vdash P\ \mathbf{Assert} \quad \Upsilon \vdash P\ \mathbf{Valid} \quad \text{(passive)}$$

$$\Upsilon \vdash x\ \mathbf{Var} \quad \Upsilon \vdash \{P\}\ C\ \{Q\}. \qquad \text{(active)}$$

Rules

The *rules* of (our slight modification of) Reddy's logic are schemas of the form

$$\frac{P_1 \quad \cdots \quad P_k}{C},$$

where the premisses P_i and the conclusion C are schematic judgements.

(An instance of) a *pre-rule* is obtained from (an instance of) a rule by deleting the permission contexts.

Trees and Proofs

A *tree* consists of a finite set Nodes, a node root $\in$ Nodes, and a function parents $\in$ Nodes $\to$ (Nodes*), satisfying conditions that insure reachability from root, and the absence of cycles and common ancestors.

A *proof* (*pre-proof*) of shape $\langle \text{Nodes}, \text{root}, \text{ parents}\rangle$ is a node-indexed family $\langle J_n \rangle$ of judgements (pre-judgements) such that, for each node n with parents $n_1, \ldots, n_k$,

$$\frac{J_{n_1} \qquad \cdots \qquad J_{n_k}}{J_n}$$

is an instance of a rule (pre-rule).

We say that a node n is *passive* (*active*) if J_n is passive (active).

Erasure and Extension

If a pre-judgement, pre-rule instance, or pre-proof X^0 is obtained from a judgement, rule instance, or proof X by deleting all permission contexts, we say that X_0 is the *erasure* of X, or that X *erases to* X^0.

If a pre-proof P^0 is obtained from a proof P by deleting all permission contexts Δ_n, we say that P *extends* P_0 with the node-indexed family $\langle \Delta_n \rangle$ of contexts.

Passive Rules

Reddy's rules with passive conclusions will be replaced by two premiss-free rules with side conditions:

$$\overline{\Delta|\Upsilon \vdash E\ \mathbf{Exp}}\ \text{ where } \forall v \in \mathsf{FV}(E).\ \Delta\ v\ \mathbf{self} > 0$$

$$\overline{\Delta|\Upsilon \vdash P\ \mathbf{Assert}}\ \text{ where } \forall v \in \mathsf{FV}(P).\ \Delta\ v\ \mathbf{self} > 0$$

$$\overline{\Delta|\Upsilon \vdash P\ \mathbf{Valid}}\ \begin{array}{l}\text{where } \forall v \in \mathsf{FV}(P).\ \Delta\ v\ \mathbf{self} > 0\\ \text{and } P \text{ is a valid assertion.}\end{array}$$

where $\mathsf{FV}(X)$ denotes the set of free variables of X.

Write Proofs

A *write-proof* is a proof in which the side conditions $\forall v \in \mathsf{FV}(X).\ \Delta\ v\ \mathbf{self} > 0$ of the passive rules are ignored, so that the permissions needed for variable reading are not checked.

The Plot (Phase I)

Given a pre-proof P^0, our algorithm should produce a proof that extends P^0, if such a proof exists. We assume that the pre-proof P^0 and its underlying tree are fixed.

In its first phase, the algorithm traverses the pre-proof from leaves to root, and computes at each node *permission restrictions* that must be satisfied by any write-proof.

Permission Restrictions

A *permission restriction* is a partial function

$$\Phi\colon \mathsf{Vars} \rightharpoonup \mathcal{P}(\mathsf{Owners}).$$

If a permission restriction is attached to a node n in a pre-proof, its domain will be the set of variables that may be assigned by the right side of the pre-judgement at n. (If n is passive, the domain will be empty.)

We say that a context Δ *satisfies* a permission restriction Φ iff

$$\forall v \in \mathrm{dom}\,\Phi.\ \textstyle\sum_{o \in \mathsf{Owners}} \Delta\, v\, o = 1$$

and

$$\forall v \in \mathrm{dom}\,\Phi, o \in \mathsf{Owners}.\ o \notin \Phi\, v \text{ implies } \Delta\, v\, o = 0.$$

As a consequence,

$$\forall v \in \mathrm{dom}\,\Phi.\ \textstyle\sum_{o \in \Phi\, v} \Delta\, v\, o = 1.$$

Note that, if there is any $v \in \mathrm{dom}\,\Phi$ such that $\Phi\, v$ is empty, then no Δ satisfies Φ.

The Permission Ordering

We impose the following preorder on permission contexts:

$$\Delta \leq \Delta' \;\text{ iff }\; \forall v \in \mathsf{Vars}, o \in \mathsf{Owners}. \\ \Delta\, v\, o > 0 \text{ implies } \Delta'\, v\, o > 0.$$

When $\Delta \leq \Delta'$, we say that Δ' is more permissive than Δ.

The Plot (Phase II)

If any permission restriction computed in the first phase is unsatisfiable, then there is no proof extending P^0.

Otherwise, in its second phase, the algorithm traverses the pre-proof from root to leaves, computing contexts that extend the pre-proof to a *maximally permissive* write-proof.

During the second phase, the algorithm checks the side-conditions on the instances of passive rules. Since, if any write-proof is a proof, the maximally permissive write-proof will be a proof, this suffices to decide whether a proof (extending P^0) exists.

An Example (The Problematic Program)

$[p\colon \mathbf{self}\colon 1] \vdash$

$\{R_1 * R_2\}$

$\mathbf{resource}\ r_1\ \mathbf{in}\ \mathbf{resource}\ r_2\ \mathbf{in}$

$(\mathbf{with}\ r_1\ \mathbf{do}\ ((\mathbf{with}\ r_2\ \mathbf{do}\ p := 0); [0] := 3))$

$\parallel (\mathbf{with}\ r_2\ \mathbf{do}\ ((\mathbf{with}\ r_1\ \mathbf{do}\ p := 1); [0] := 4))$

$\{R_1 * R_2\}$

$$\mathsf{Vars} = \{p\}$$
$$\mathsf{Owners} = \{r_1, r_2, \mathbf{self}\}.$$

The Resource Invariants

$$R_1 = \textbf{if } p = 0 \textbf{ then } 0 \mapsto 3 \textbf{ else emp}$$
$$R_2 = \textbf{if } p = 0 \textbf{ then emp else } 0 \mapsto 4.$$

Thus

$$\begin{aligned}
&R_1 * R_2 \\
&\quad \text{iff } \textbf{if } p = 0 \textbf{ then } 0 \mapsto 3 * \textbf{emp else emp} * 0 \mapsto 4 \\
&\quad \text{iff } \textbf{if } p = 0 \textbf{ then } 0 \mapsto 3 \textbf{ else } 0 \mapsto 4 \\
&\quad \text{implies } 0 \mapsto -
\end{aligned}$$

and

$$p = 0 \wedge R_1 \text{ iff } p = 0 \wedge 0 \mapsto 3$$
$$p = 0 \wedge R_2 \text{ iff } p = 0 \wedge \textbf{emp}$$
$$p \neq 0 \wedge R_1 \text{ iff } p \neq 0 \wedge \textbf{emp}$$
$$p \neq 0 \wedge R_2 \text{ iff } p \neq 0 \wedge 0 \mapsto 4.$$

Using the Rule for (Assignable) Variables

$$\frac{}{p\colon[\mathbf{self}\colon 1] \vdash p\ \mathbf{Var}} \qquad \Phi = [p\colon\{\mathbf{self}\}]$$

Using the Rule for Assignment

$$\frac{\begin{array}{c}\Delta \vdash p\ \mathbf{Var} \\ \Delta \vdash 0\ \mathbf{Exp} \\ \Delta \vdash 0 \mapsto - \wedge p = 0\ \mathbf{Assert}\end{array}}{\begin{array}{l}\Delta \vdash \{0 \mapsto - \wedge 0 = 0\} \\ \qquad p := 0 \\ \qquad \{0 \mapsto - \wedge p = 0\}\end{array}} \qquad \begin{array}{l}\Phi_1 = [p\colon\{\mathbf{self}\}] \\ \Phi_2 = [\,] \\ \Phi_3 = [\,] \\ \\ \Phi = [p\colon\{\mathbf{self}\}]\end{array}$$

Using the Rule of Consequence

$$\dfrac{\begin{array}{ll} \Delta \vdash R_1 \ast R_2 \Rightarrow 0 \mapsto - \wedge 0 = 0 \ \mathbf{Valid} & \Phi_1 = [\,] \\ \quad \Delta \vdash \{0 \mapsto - \wedge 0 = 0\} & \\ \qquad p := 0 & \Phi_2 = [p\colon \{\mathbf{self}\}] \\ \qquad \{0 \mapsto - \wedge p = 0\} & \\ \Delta \vdash 0 \mapsto - \wedge p = 0 \Rightarrow & \\ \qquad R_2 \ast (0 \mapsto - \wedge p = 0) \ \mathbf{Valid} & \Phi_3 = [\,] \end{array}}{\begin{array}{ll} \Delta \vdash \{R_1 \ast R_2\} & \\ \qquad p := 0 & \Phi = [p\colon \{\mathbf{self}\}] \\ \qquad \{R_2 \ast (0 \mapsto - \wedge p = 0)\} & \end{array}}$$

An (Unconditional) Critical Region

$$\Delta | r_2 \colon R_2 \vdash R_1 \ \mathbf{Assert} \qquad \Phi_1 = [\,]$$

$$\Delta | r_2 \colon R_2 \vdash 0 \mapsto - \wedge p = 0 \ \mathbf{Assert} \qquad \Phi_2 = [\,]$$

$$\frac{\begin{array}{l}\Delta' \vdash \{R_1 \ * \ R_2\} \\ \qquad p := 0 \\ \qquad \{R_2 \ * \ (0 \mapsto - \wedge p = 0)\}\end{array}}{\begin{array}{l}\Delta | r_2 \colon R_2 \vdash \{R_1\} \\ \qquad \mathbf{with}\ r_2\ \mathbf{do}\ p := 0 \\ \qquad \{0 \mapsto - \wedge p = 0\}\end{array}} \qquad \begin{array}{l}\Phi_3 = [p \colon \{\mathbf{self}\}] \\ \\ \Phi = [p \colon \{r_2, \mathbf{self}\}]\end{array}$$

where

$$\begin{aligned}\Delta'\, p\, o &= \Delta\, p\, o \text{ when } o \notin \{r_2, \mathbf{self}\} \\ \Delta'\, p\ \mathbf{self} &= \Delta\, p\ \mathbf{self} + \Delta\, p\, r_2 \leq 1 \\ \Delta'\, p\, r_2 &= 0.\end{aligned}$$

From Φ_3, we have $\Delta'\, p\, o = \mathbf{if}\ o = \mathbf{self}\ \mathbf{then}\ 1\ \mathbf{else}\ 0$, so that

$$\Delta\, p\, o = \mathbf{if}\ o = \mathbf{self}\ \mathbf{then}\ \pi_1\ \mathbf{else}\ \mathbf{if}\ o = r_2\ \mathbf{then}\ \pi_2\ \mathbf{else}\ 0,$$

where $\pi_1 + \pi_2 = 1$. Thus $\Phi = [p \colon \{r_2, \mathbf{self}\}]$.

Mutation

$$\frac{\begin{array}{ll} \Delta | r_2 \colon R_2 \vdash 0 \ \mathbf{Exp} & \Phi_1 = [\,] \\ \Delta | r_2 \colon R_2 \vdash 3 \ \mathbf{Exp} & \Phi_2 = [\,] \end{array}}{\begin{array}{ll} \Delta | r_2 \colon R_2 \vdash \{0 \mapsto - \wedge p = 0\} & \\ \qquad [0] := 3 & \Phi = [\,] \\ \qquad \{0 \mapsto 3 \wedge p = 0\} & \end{array}}$$

Sequential Composition

$$\frac{\begin{array}{ll} \Delta | r_2 \colon R_2 \vdash \{R_1\} & \\ \qquad \mathbf{with}\ r_2\ \mathbf{do}\ p := 0 & \Phi_1 = [p \colon \{r_2, \mathbf{self}\}] \\ \qquad \{0 \mapsto - \wedge p = 0\} & \\ \Delta | r_2 \colon R_2 \vdash \{0 \mapsto - \wedge p = 0\} & \\ \qquad [0] := 3 & \Phi_2 = [\,] \\ \qquad \{0 \mapsto 3 \wedge p = 0\} & \end{array}}{\begin{array}{ll} \Delta | r_2 \colon R_2 \vdash \{R_1\} & \\ \qquad \mathbf{with}\ r_2\ \mathbf{do}\ p := 0\,; & \\ \qquad [0] := 3 & \Phi = [p \colon \{r_2, \mathbf{self}\}] \\ \qquad \{0 \mapsto 3 \wedge p = 0\} & \end{array}}$$

Consequence

$$\Delta | r_2 \colon R_2 \vdash \begin{array}{l} \{R_1\} \\ \textbf{with } r_2 \textbf{ do } p := 0\,; \\ [0] := 3 \\ \{0 \mapsto 3 \wedge p = 0\} \end{array} \qquad \Phi_1 = [p \colon \{r_2, \textbf{self}\}]$$

$$\frac{\Delta | r_2 \colon R_2 \vdash 0 \mapsto 3 \wedge p = 0 \Rightarrow R_1 \textbf{ Valid}}{} \qquad \Phi_2 = [\,]$$

$$\Delta | r_2 \colon R_2 \vdash \begin{array}{l} \{R_1\} \\ \textbf{with } r_2 \textbf{ do } p := 0\,; \\ [0] := 3 \\ \{R_1\} \end{array} \qquad \Phi = [p \colon \{r_2, \textbf{self}\}]$$

Another Critical Region

$$\Delta | r_1 \colon R_1, r_2 \colon R_2 \vdash \textbf{emp Assert} \qquad \Phi_1 = [\,]$$

$$\Delta | r_1 \colon R_1, r_2 \colon R_2 \vdash \textbf{emp Assert} \qquad \Phi_2 = [\,]$$

$$\begin{array}{ll} \Delta' | r_2 \colon R_2 \vdash & \{R_1\} \\ & \textbf{with}\ r_2\ \textbf{do}\ p := 0\ ; \\ & [0] := 3 \\ & \{R_1\} \end{array} \qquad \Phi_3 = [p \colon \{r_2, \textbf{self}\}]$$

$$\overline{\begin{array}{ll} \Delta | r_1 \colon R_1, r_2 \colon R_2 \vdash & \{\textbf{emp}\} \\ & \textbf{with}\ r_1\ \textbf{do}\,(\\ & \quad \textbf{with}\ r_2\ \textbf{do}\ p := 0\ ; \\ & \quad [0] := 3) \\ & \{\textbf{emp}\} \end{array}} \qquad \begin{array}{l} \Phi = \\ \quad [p \colon \{r_1, r_2, \textbf{self}\}] \end{array}$$

where

$$\begin{aligned} \Delta'\, p\, o &= \Delta\, p\, o \text{ when } o \notin \{r_1, \textbf{self}\} \\ \Delta'\, p\, \textbf{self} &= \Delta\, p\, \textbf{self} + \Delta\, p\, r_1 \leq 1 \\ \Delta'\, p\, r_1 &= 0. \end{aligned}$$

From $\Delta'\, p\, r_1 = 0$, we obtain $\Phi_3 = [p \colon \{r_2, \textbf{self}\}]$.

Similarly

$$\Delta | r_1 \colon R_1, r_2 \colon R_2 \vdash \begin{array}{l} \{\mathbf{emp}\} \\ \mathbf{with}\ r_2\ \mathbf{do}\,(\\ \quad \mathbf{with}\ r_1\ \mathbf{do}\ p := 1\ ; \\ \quad [0] := 4) \\ \{\mathbf{emp}\} \end{array} \qquad \begin{array}{l} \Phi = \\ \quad [p \colon \{r_1, r_2, \mathbf{self}\}] \end{array}$$

Parallel Composition

$$
\begin{array}{rl}
\Delta_1 | r_1 \colon R_1, r_2 \colon R_2 \vdash & \{\mathbf{emp}\} \qquad\qquad \Phi_1 = [p \colon \{r_1, r_2, \mathbf{self}\}] \\
& \mathbf{with}\ r_1\ \mathbf{do}\,(\mathbf{with}\ r_2\ \mathbf{do}\ p := 0\ ;\ [0] := 3) \\
& \{\mathbf{emp}\}
\end{array}
$$

$$
\begin{array}{rl}
\Delta_2 | r_1 \colon R_1, r_2 \colon R_2 \vdash & \{\mathbf{emp}\} \qquad\qquad \Phi_2 = [p \colon \{r_1, r_2, \mathbf{self}\}] \\
& \mathbf{with}\ r_2\ \mathbf{do}\,(\mathbf{with}\ r_1\ \mathbf{do}\ p := 1\ ;\ [0] := 4) \\
& \{\mathbf{emp}\}
\end{array}
$$

$$
\begin{array}{rl}
\Delta | r_1 \colon R_1, r_2 \colon R_2 \vdash & \{\mathbf{emp} * \mathbf{emp}\} \qquad\qquad \Phi = [p \colon \{r_1, r_2\}] \\
& \mathbf{with}\ r_1\ \mathbf{do}\,(\mathbf{with}\ r_2\ \mathbf{do}\ p := 0\ ;\ [0] := 3) \\
& \quad \| \\
& \mathbf{with}\ r_2\ \mathbf{do}\,(\mathbf{with}\ r_1\ \mathbf{do}\ p := 1\ ;\ [0] := 4) \\
& \{\mathbf{emp} * \mathbf{emp}\}
\end{array}
$$

where

$$
\begin{aligned}
\Delta_1\, p &= [r_1 \colon \pi_1, r_2 \colon \pi_2, \mathbf{self} \colon \pi_s] \\
\Delta_2\, p &= [r_1 \colon \pi_1, r_2 \colon \pi_2, \mathbf{self} \colon \pi'_s] \\
\Delta\, p &= [r_1 \colon \pi_1, r_2 \colon \pi_2, \mathbf{self} \colon \pi_s + \pi'_s],
\end{aligned}
$$

so that

$$
\begin{aligned}
\pi_1 + \pi_2 + \pi_s &= 1 \\
\pi_1 + \pi_2 + \pi'_s &= 1 \\
\pi_1 + \pi_2 + \pi_s + \pi'_s &\leq 1,
\end{aligned}
$$

which implies that $\pi_s = \pi'_s = \pi_s + \pi'_s = 0$. Thus $\Phi = [p \colon \{r_1, r_2\}]$.

Resource Declaration

$$\dfrac{\begin{array}{ll} \Delta_1 | r_1 \colon R_1 \vdash R_2 \ \mathbf{Assert} & \Phi_1 = [\,] \\ \Delta_2 | r_1 \colon R_1, r_2 \colon R_2 \vdash \begin{array}[t]{l} \{\mathbf{emp} * \mathbf{emp}\} \\ \mathbf{with}\ r_1\ \mathbf{do}\,(\mathbf{with}\ r_2\ \mathbf{do}\ p := 0\ ;\ [0] := 3) \\ \quad \| \\ \mathbf{with}\ r_2\ \mathbf{do}\,(\mathbf{with}\ r_1\ \mathbf{do}\ p := 1\ ;\ [0] := 4) \\ \{\mathbf{emp} * \mathbf{emp}\} \end{array} & \Phi_2 = [p \colon \{r_1, r_2\}] \end{array}}{\begin{array}{ll} \Delta | r_1 \colon R_1 \vdash \begin{array}[t]{l} \{\mathbf{emp} * \mathbf{emp} * R_2\} \\ \mathbf{resource}\ r_2\ \mathbf{in} \\ \quad \mathbf{with}\ r_1\ \mathbf{do}\,(\mathbf{with}\ r_2\ \mathbf{do}\ p := 0\ ;\ [0] := 3) \\ \qquad \| \\ \quad \mathbf{with}\ r_2\ \mathbf{do}\,(\mathbf{with}\ r_1\ \mathbf{do}\ p := 1\ ;\ [0] := 4) \\ \{\mathbf{emp} * \mathbf{emp} * R_2\} \end{array} & \Phi = [p \colon \{r_1, \mathbf{self}\}] \end{array}}$$

where

$$\begin{aligned} \Delta_2\, p &= [r_1 \colon \pi_1, r_2 \colon \pi_2, \mathbf{self} \colon \pi_s] \\ \Delta_1\, p &= [\mathbf{self} \colon \pi_2] \\ \Delta\, p &= [r_1 \colon \pi_1, r_2 \colon 0, \mathbf{self} \colon \pi_s + \pi_2]. \end{aligned}$$

Thus $\Phi = [p \colon \{r_1, \mathbf{self}\}]$.

Another Resource Declaration

$$\Delta_1 \vdash R_1 \;\mathbf{Assert} \qquad\qquad \Phi_1 = [\,]$$

$$\begin{array}{ll} \Delta_2|r_1\colon R_1 \vdash & \{\mathbf{emp} * \mathbf{emp} * R_2\} \qquad\qquad \Phi_2 = [p\colon \{r_1, \mathbf{self}\}] \\ & \mathbf{resource}\; r_2\; \mathbf{in} \\ & \quad \mathbf{with}\; r_1\; \mathbf{do}\,(\mathbf{with}\; r_2\; \mathbf{do}\; p := 0\,;\, [0] := 3) \\ & \qquad \| \\ & \quad \mathbf{with}\; r_2\; \mathbf{do}\,(\mathbf{with}\; r_1\; \mathbf{do}\; p := 1\,;\, [0] := 4) \\ & \{\mathbf{emp} * \mathbf{emp} * R_2\} \end{array}$$

$$\begin{array}{l} \Delta \vdash \{\mathbf{emp} * \mathbf{emp} * R_1 * R_2\} \qquad\qquad \Phi = [p\colon \{\mathbf{self}\}] \\ \quad \mathbf{resource}\; r_1\; \mathbf{in}\; \mathbf{resource}\; r_2\; \mathbf{in} \\ \qquad \mathbf{with}\; r_1\; \mathbf{do}\,(\mathbf{with}\; r_2\; \mathbf{do}\; p := 0\,;\, [0] := 3) \\ \qquad\quad \| \\ \qquad \mathbf{with}\; r_2\; \mathbf{do}\,(\mathbf{with}\; r_1\; \mathbf{do}\; p := 1\,;\, [0] := 4) \\ \quad \{\mathbf{emp} * \mathbf{emp} * R_1 * R_2\} \end{array}$$

where

$$\begin{aligned} \Delta_2\, p &= [r_1\colon \pi_1, r_2\colon \pi_2, \mathbf{self}\colon \pi_s] \\ \Delta_1\, p &= [\mathbf{self}\colon \pi_1] \\ \Delta\, p &= [r_1\colon 0, r_2\colon \pi_2, \mathbf{self}\colon \pi_s + \pi_1]. \end{aligned}$$

But by Φ_2, $\pi_2 = 0$. Thus $\Phi = [p\colon \{\mathbf{self}\}]$.

At the Root

We take $\Delta^{\mathsf{max}}_{\mathsf{root}}$ to be the maximally permissive context that satisfies $\Phi_{\mathsf{root}} = [p\colon \{\mathbf{self}\}]$:

$$\Delta^{\mathsf{max}}_{\mathsf{root}}\, p = [\mathbf{self} : 1].$$

Then we go backwards through our proof.

Passive judgement whose side conditions hold (either because $\Delta^{\mathsf{max}}\, p\, \mathbf{self} > 0$ or because p is not a free variable) are marked with an asterisk.

Another Resource Declaration

$$\dfrac{\begin{array}{ll} *\Delta_1 \vdash R_1 \ \textbf{Assert} & \Phi_1 = [\,] \\ \Delta_2 | r_1 \colon R_1 \vdash \{\mathbf{emp} * \mathbf{emp} * R_2\} & \Phi_2 = [p \colon \{r_1, \mathbf{self}\}] \\ \quad \mathbf{resource}\ r_2\ \mathbf{in} & \\ \quad\quad \mathbf{with}\ r_1\ \mathbf{do}\,(\mathbf{with}\ r_2\ \mathbf{do}\ p := 0\ ; [0] := 3) & \\ \quad\quad\quad \| & \\ \quad\quad \mathbf{with}\ r_2\ \mathbf{do}\,(\mathbf{with}\ r_1\ \mathbf{do}\ p := 1\ ; [0] := 4) & \\ \quad \{\mathbf{emp} * \mathbf{emp} * R_2\} & \end{array}}{\begin{array}{ll} \Delta \vdash \{\mathbf{emp} * \mathbf{emp} * R_1 * R_2\} & \Phi = [p \colon \{\mathbf{self}\}] \\ \quad \mathbf{resource}\ r_1\ \mathbf{in}\ \mathbf{resource}\ r_2\ \mathbf{in} & \\ \quad\quad \mathbf{with}\ r_1\ \mathbf{do}\,(\mathbf{with}\ r_2\ \mathbf{do}\ p := 0\ ; [0] := 3) & \\ \quad\quad\quad \| & \\ \quad\quad \mathbf{with}\ r_2\ \mathbf{do}\,(\mathbf{with}\ r_1\ \mathbf{do}\ p := 1\ ; [0] := 4) & \\ \quad \{\mathbf{emp} * \mathbf{emp} * R_1 * R_2\} & \end{array}}$$

where

$$\begin{aligned} \Delta_2\, p &= [r_1 \colon \pi_1, r_2 \colon \pi_2, \mathbf{self} \colon \pi_s] \\ \Delta_1\, p &= [\mathbf{self} \colon \pi_1] \\ \Delta\, p &= [r_1 \colon 0, r_2 \colon \pi_2, \mathbf{self} \colon \pi_s + \pi_1]. \end{aligned}$$

From $\Delta^{\max} p = [\mathbf{self} : 1]$, we get $\pi_2 = 0$ and $\pi_s + \pi_1 = 1$. Choosing $\pi_s = \pi_1 = \frac{1}{2}$, we have

$$\Delta_1^{\max} p = [\mathbf{self} \colon \tfrac{1}{2}] \qquad \Delta_2^{\max} p = [r_1 \colon \tfrac{1}{2}, \mathbf{self} \colon \tfrac{1}{2}]$$

Resource Declaration

$$\frac{\begin{array}{ll} *\Delta_1|r_1{:}\,R_1 \vdash R_2\ \mathbf{Assert} & \Phi_1 = [\,] \\ \Delta_2|r_1{:}\,R_1, r_2{:}\,R_2 \vdash \{\mathbf{emp} * \mathbf{emp}\} & \Phi_2 = [p{:}\,\{r_1, r_2\}] \\ \quad \mathbf{with}\ r_1\ \mathbf{do}\,(\mathbf{with}\ r_2\ \mathbf{do}\ p := 0\ ;\ [0] := 3) & \\ \quad\quad \| & \\ \quad \mathbf{with}\ r_2\ \mathbf{do}\,(\mathbf{with}\ r_1\ \mathbf{do}\ p := 1\ ;\ [0] := 4) & \\ \quad \{\mathbf{emp} * \mathbf{emp}\} & \end{array}}{\begin{array}{ll} \Delta|r_1{:}\,R_1 \vdash \{\mathbf{emp} * \mathbf{emp} * R_2\} & \Phi = [p{:}\,\{r_1, \mathbf{self}\}] \\ \quad \mathbf{resource}\ r_2\ \mathbf{in} & \\ \quad\quad \mathbf{with}\ r_1\ \mathbf{do}\,(\mathbf{with}\ r_2\ \mathbf{do}\ p := 0\ ;\ [0] := 3) & \\ \quad\quad\quad \| & \\ \quad\quad \mathbf{with}\ r_2\ \mathbf{do}\,(\mathbf{with}\ r_1\ \mathbf{do}\ p := 1\ ;\ [0] := 4) & \\ \quad \{\mathbf{emp} * \mathbf{emp} * R_2\} & \end{array}}$$

where

$$\begin{aligned} \Delta_2\, p &= [r_1{:}\,\pi_1, r_2{:}\,\pi_2, \mathbf{self}{:}\,\pi_s] \\ \Delta_1\, p &= [\mathbf{self}{:}\,\pi_2] \\ \Delta\, p &= [r_1{:}\,\pi_1, r_2{:}\,0, \mathbf{self}{:}\,\pi_s + \pi_2]. \end{aligned}$$

From $\Delta^{\max} p = [r_1{:}\,\frac{1}{2}, \mathbf{self}{:}\,\frac{1}{2}]$, we get $\pi_1 = \frac{1}{2}$ and $\pi_s + \pi_2 = \frac{1}{2}$. But $\Phi_2\, p$ forces $\pi_s = 0$, so that $\pi_2 = \frac{1}{2}$ and

$$\Delta_1^{\max} p = [\mathbf{self}{:}\,\tfrac{1}{2}] \qquad \Delta_2^{\max} p = [r_1{:}\,\tfrac{1}{2}, r_2{:}\,\tfrac{1}{2}].$$

Parallel Composition

$$\frac{\begin{array}{ll}\Delta_1|r_1\colon R_1, r_2\colon R_2 \vdash \{\mathbf{emp}\} & \Phi_1 = [p\colon\{r_1, r_2, \mathbf{self}\}] \\ \quad \mathbf{with}\ r_1\ \mathbf{do}\,(\mathbf{with}\ r_2\ \mathbf{do}\ p := 0\ ;\ [0] := 3) & \\ \quad \{\mathbf{emp}\} & \\ \Delta_2|r_1\colon R_1, r_2\colon R_2 \vdash \{\mathbf{emp}\} & \Phi_2 = [p\colon\{r_1, r_2, \mathbf{self}\}] \\ \quad \mathbf{with}\ r_2\ \mathbf{do}\,(\mathbf{with}\ r_1\ \mathbf{do}\ p := 1\ ;\ [0] := 4) & \\ \quad \{\mathbf{emp}\} & \end{array}}{\begin{array}{ll}\Delta|r_1\colon R_1, r_2\colon R_2 \vdash \{\mathbf{emp} * \mathbf{emp}\} & \Phi = [p\colon\{r_1, r_2\}] \\ \quad \mathbf{with}\ r_1\ \mathbf{do}\,(\mathbf{with}\ r_2\ \mathbf{do}\ p := 0\ ;\ [0] := 3) & \\ \qquad \| & \\ \quad \mathbf{with}\ r_2\ \mathbf{do}\,(\mathbf{with}\ r_1\ \mathbf{do}\ p := 1\ ;\ [0] := 4) & \\ \quad \{\mathbf{emp} * \mathbf{emp}\} & \end{array}}$$

where

$$\begin{aligned}\Delta_1\, p &= [r_1\colon \pi_1, r_2\colon \pi_2, \mathbf{self}\colon \pi_s] \\ \Delta_2\, p &= [r_1\colon \pi_1, r_2\colon \pi_2, \mathbf{self}\colon \pi'_s] \\ \Delta\, p &= [r_1\colon \pi_1, r_2\colon \pi_2, \mathbf{self}\colon \pi_s + \pi'_s].\end{aligned}$$

From $\Delta^{\mathsf{max}} p = [r_1\colon \frac{1}{2}, r_2\colon \frac{1}{2}]$, we find that $\pi_s = 0$ and $\pi'_s = 0$, and

$$\Delta_1^{\mathsf{max}} p = \Delta_2^{\mathsf{max}} p = \Delta^{\mathsf{max}} p.$$

Another Critical Region

$$*\Delta|r_1\colon R_1, r_2\colon R_2 \vdash \textbf{emp Assert} \qquad \Phi_1 = [\,]$$

$$*\Delta|r_1\colon R_1, r_2\colon R_2 \vdash \textbf{emp Assert} \qquad \Phi_2 = [\,]$$

$$\Delta'|r_2\colon R_2 \vdash \begin{array}{l}\{R_1\}\\ \textbf{with } r_2 \textbf{ do } p := 0\ ;\\ [0] := 3\\ \{R_1\}\end{array} \qquad \Phi_3 = [p\colon \{r_2, \textbf{self}\}]$$

$$\overline{\Delta|r_1\colon R_1, r_2\colon R_2 \vdash \begin{array}{l}\{\textbf{emp}\}\\ \textbf{with } r_1 \textbf{ do} \,(\\ \quad \textbf{with } r_2 \textbf{ do } p := 0\ ;\\ \quad [0] := 3)\\ \{\textbf{emp}\}\end{array}} \qquad \begin{array}{l}\Phi =\\ \quad [p\colon \{r_1, r_2, \textbf{self}\}]\end{array}$$

where

$$\begin{aligned} \Delta'\, p\, o &= \Delta\, p\, o \text{ when } o \notin \{r_1, \textbf{self}\} \\ \Delta'\, p\, \textbf{self} &= \Delta\, p\, \textbf{self} + \Delta\, p\, r_1 \leq 1 \\ \Delta'\, p\, r_1 &= 0. \end{aligned}$$

From $\Delta^{\mathsf{max}}\, p = [r_1\colon \frac{1}{2}, r_2\colon \frac{1}{2}]$ we get

$$\Delta^{\mathsf{max}\prime}\, p = [r_2\colon \tfrac{1}{2}, \textbf{self}\colon \tfrac{1}{2}].$$

Consequence

$$
\begin{array}{ll}
\begin{array}{rl}
\Delta | r_2 \colon R_2 \vdash & \{R_1\} \\
& \textbf{with } r_2 \textbf{ do } p := 0\ ; \\
& [0] := 3 \\
& \{0 \mapsto 3 \wedge p = 0\}
\end{array} & \Phi_1 = [p\colon \{r_2, \textbf{self}\}] \\
* \Delta | r_2 \colon R_2 \vdash 0 \mapsto 3 \wedge p = 0 \Rightarrow R_1 \textbf{ Valid} & \Phi_2 = [\,] \\
\hline
\begin{array}{rl}
\Delta | r_2 \colon R_2 \vdash & \{R_1\} \\
& \textbf{with } r_2 \textbf{ do } p := 0\ ; \\
& [0] := 3 \\
& \{R_1\}
\end{array} & \Phi = [p\colon \{r_2, \textbf{self}\}]
\end{array}
$$

Obviously, Δ^{max} is preserved.

Mutation

$$\frac{\begin{array}{ll} *\Delta | r_2 \colon R_2 \vdash 0\ \mathbf{Exp} & \Phi_1 = [\,] \\ *\Delta | r_2 \colon R_2 \vdash 3\ \mathbf{Exp} & \Phi_2 = [\,] \end{array}}{\begin{array}{ll} \Delta | r_2 \colon R_2 \vdash \{0 \mapsto - \wedge p = 0\} & \\ \qquad [0] := 3 & \Phi = [\,] \\ \qquad \{0 \mapsto 3 \wedge p = 0\} & \end{array}}$$

Obviously, Δ^{max} is preserved.

Sequential Composition

$$\frac{\begin{array}{ll} \Delta | r_2 \colon R_2 \vdash \{R_1\} & \\ \qquad \mathbf{with}\ r_2\ \mathbf{do}\ p := 0 & \Phi_1 = [p \colon \{r_2, \mathbf{self}\}] \\ \qquad \{0 \mapsto - \wedge p = 0\} & \\ *\Delta | r_2 \colon R_2 \vdash \{0 \mapsto - \wedge p = 0\} & \\ \qquad [0] := 3 & \Phi_2 = [\,] \\ \qquad \{0 \mapsto 3 \wedge p = 0\} & \end{array}}{\begin{array}{ll} \Delta | r_2 \colon R_2 \vdash \{R_1\} & \\ \qquad \mathbf{with}\ r_2\ \mathbf{do}\ p := 0\ ; & \Phi = [p \colon \{r_2, \mathbf{self}\}] \\ \qquad [0] := 3 & \\ \qquad \{0 \mapsto 3 \wedge p = 0\} & \end{array}}$$

Obviously, Δ^{max} is preserved.

An (Unconditional) Critical Region

$$*\Delta|r_2\colon R_2 \vdash R_1 \ \mathbf{Assert} \qquad \Phi_1 = [\,]$$

$$*\Delta|r_2\colon R_2 \vdash 0 \mapsto - \wedge p = 0 \ \mathbf{Assert} \qquad \Phi_2 = [\,]$$

$$\frac{\begin{array}{ll} \Delta' \vdash & \{R_1 \, * \, R_2\} \\ & p := 0 \\ & \{R_2 \, * \, (0 \mapsto - \wedge p = 0)\} \end{array} \qquad \Phi_3 = [p\colon \{\mathbf{self}\}]}{\begin{array}{ll} \Delta|r_2\colon R_2 \vdash & \{R_1\} \\ & \mathbf{with}\ r_2\ \mathbf{do}\ p := 0 \\ & \{0 \mapsto - \wedge p = 0\} \end{array} \qquad \Phi = [p\colon \{r_2, \mathbf{self}\}]}$$

where

$$\begin{aligned} \Delta'\, p\, o &= \Delta\, p\, o \text{ when } o \notin \{r_2, \mathbf{self}\} \\ \Delta'\, p\ \mathbf{self} &= \Delta\, p\ \mathbf{self} + \Delta\, p\, r_2 \leq 1 \\ \Delta'\, p\, r_2 &= 0. \end{aligned}$$

From $\Delta^{\mathsf{max}}\, p = [r_2\colon \frac{1}{2}, \mathbf{self}\colon \frac{1}{2}]$, we get

$$\Delta^{\mathsf{max}\prime}\, p = [\mathbf{self}\colon 1].$$

Using the Rule of Consequence

$$*\boldsymbol{\Delta} \vdash R_1 \,*\, R_2 \Rightarrow 0 \mapsto - \wedge 0 = 0 \ \textbf{Valid} \qquad \Phi_1 = [\,]$$

$$\begin{array}{l} \boldsymbol{\Delta} \vdash \{0 \mapsto - \wedge 0 = 0\} \\ \qquad p := 0 \\ \qquad \{0 \mapsto - \wedge p = 0\} \end{array} \qquad \Phi_2 = [p\colon \{\textbf{self}\}]$$

$$\begin{array}{l} *\boldsymbol{\Delta} \vdash 0 \mapsto - \wedge p = 0 \Rightarrow \\ \qquad R_2 \,*\, (0 \mapsto - \wedge p = 0) \ \textbf{Valid} \end{array} \qquad \Phi_3 = [\,]$$

$$\frac{}{\begin{array}{l} \boldsymbol{\Delta} \vdash \{R_1 \,*\, R_2\} \\ \qquad p := 0 \\ \qquad \{R_2 \,*\, (0 \mapsto - \wedge p = 0)\} \end{array}} \qquad \Phi = [p\colon \{\textbf{self}\}]$$

Obviously, $\boldsymbol{\Delta}^{\mathsf{max}}$ is preserved.

Using the Rule for (Assignable) Variables

$$\frac{}{p\colon[\mathbf{self}\colon 1] \vdash p\ \mathbf{Var}} \qquad \Phi = [p\colon\{\mathbf{self}\}]$$

which is satisfied by $\Delta^{\mathsf{max}}\,p = [\mathbf{self}\colon 1]$.

Using the Rule for Assignment

$$\frac{\begin{array}{ll} \Delta \vdash p\ \mathbf{Var} & \Phi_1 = [p\colon\{\mathbf{self}\}] \\ *\Delta \vdash 0\ \mathbf{Exp} & \Phi_2 = [\,] \\ *\Delta \vdash 0 \mapsto - \wedge p = 0\ \mathbf{Assert} & \Phi_3 = [\,] \end{array}}{\begin{array}{ll} \Delta \vdash \{0 \mapsto - \wedge 0 = 0\} & \\ \quad p := 0 & \Phi = [p\colon\{\mathbf{self}\}] \\ \quad \{0 \mapsto - \wedge p = 0\} & \end{array}}$$

Obviously, Δ^{max} is preserved.

At each Node during Phase I

Consider a node n in P^0 whose parents are $n_1, \ldots, n_k$. The judgements at these nodes will form an instance of a pre-rule:

$$R^0\colon \frac{\Upsilon_{n_1} \vdash S_{n_1} \quad \cdots \quad \Upsilon_{n_k} \vdash S_{n_k}}{\Upsilon_n \vdash S_n.}$$

During Phase I, the algorithm will accept permission restrictions $\Phi_{n_1}, \ldots, \Phi_{n_k}$ and will produce a permission restriction Φ_n such that

(1) If

$$\frac{\Delta_{n_1}|\Upsilon_{n_1} \vdash S_{n_1} \quad \cdots \quad \Delta_{n_k}|\Upsilon_{n_k} \vdash S_{n_k}}{\Delta_n|\Upsilon_n \vdash S_n.}$$

is a rule instance that erases to R^0, and if Δ_{n_i} satisfies Φ_{n_i} for $1 \leq i \leq k$, then Δ_n will satisfy Φ_n.

The Result of Phase I

In Phase I, the algorithm will produce a permission restriction Φ_n for each node n in P^0.

By structural induction on P^0, using (1):

(2) If P^w is a write-proof that extends P^0 with contexts $\langle \Delta_n \rangle$, then each Δ_n satisfies Φ_n.

At the Root

In Phase II, the algorithm will search for a proof whose root judgement contains the context $\Delta^{\mathsf{max}}_{\mathsf{root}}$, which must satisfy Φ_{root}. There are two cases:

Specified Root Context: We take $\Delta^{\mathsf{max}}_{\mathsf{root}}$ to be the specified root context, providing it satisfies Φ_{root}. Otherwise, by (2), there is no write-proof (and therefore no proof) that extends P^0 and has the specified root context.

Arbitrary Root Context: If, for every v in $\mathsf{dom}\,\Phi_{\mathsf{root}}$, $\Phi_{\mathsf{root}}\,v$ is nonempty, then we take $\Delta^{\mathsf{max}}_{\mathsf{root}}$ to be

$$\Delta^{\mathsf{max}}_{\mathsf{root}}\,v\,o = \begin{cases} \mathbf{if}\ v \in \mathsf{dom}\,\Phi_{\mathsf{root}}\ \mathbf{then} \\ \qquad \mathbf{if}\ o \in \Phi_{\mathsf{root}}\,v\ \mathbf{then}\ 1/\#\Phi_{\mathsf{root}}\,v\ \mathbf{else}\ 0 \\ \mathbf{else}\ 1/(\#\mathsf{Owners} + 1) \end{cases}$$

(where $\#S$ is the size of S), which is (one of) the most permissive contexts satisfying Φ_{root}.

On the other hand, if there is some variable v such that $\Phi_{\mathsf{root}}\,v$ is empty, then there is no root context satsifying Φ_{root}, and by (2), no proof extends P^0.

At each Node during Phase II

During Phase II, the algorithm will accept a context Δ_n^{max} that satisfies Φ_n and will produce contexts $\Delta_{n_1}^{\mathsf{max}}, \ldots, \Delta_{n_k}^{\mathsf{max}}$ such that

(3) Each $\Delta_{n_i}^{\mathsf{max}}$ satisfies Φ_{n_i} and

$$\frac{\Delta_{n_1}^{\mathsf{max}} | \Upsilon_{n_1} \vdash S_{n_1} \ \cdots \ \Delta_{n_k}^{\mathsf{max}} | \Upsilon_{n_k} \vdash S_{n_k}}{\Delta_n^{\mathsf{max}} | \Upsilon_n \vdash S_n.}$$

is a rule instance that erases to R^0. Moreover,

(4) If $\Delta_{n_1}, \ldots, \Delta_{n_k}$, and Δ_n satisfy $\Phi_{n_1}, \ldots, \Phi_{n_k}$, and Φ_n respectively,

$$\frac{\Delta_{n_1} | \Upsilon_{n_1} \vdash S_{n_1} \ \cdots \ \Delta_{n_k} | \Upsilon_{n_k} \vdash S_{n_k}}{\Delta_n | \Upsilon_n \vdash S_n}$$

is a rule instance that erases to R^0, and $\Delta_n \leq \Delta_n^{\mathsf{max}}$, then $\Delta_{n_i} \leq \Delta_{n_i}^{\mathsf{max}}$ for $1 \leq i \leq k$.

The Result of Phase II

In Phase II, given a context $\Delta^{\mathsf{max}}_{\mathsf{root}}$ satisfying Φ_{root}, the algorithm will produce a context Δ^{max}_n for each node n.

By induction on distance from the root, using (3):

(5) There is a write-proof that extends P^0 with $\langle \Delta^{\mathsf{max}}_n \rangle$.

Moreover, using (2), and then induction on distance from the root, using (4):

(6) If there is a write-proof that extends P^0 with $\langle \Delta_n \rangle$, and $\Delta_{\mathsf{root}} \leq \Delta^{\mathsf{max}}_{\mathsf{root}}$, then $\Delta_n \leq \Delta^{\mathsf{max}}_n$ for each node n.

The Finale

In Phase II, while generating the Δ_n^{max}, the algorithm can check whether, at all passive nodes, the side conditions of the rules

$$\overline{\Delta|\Upsilon \vdash E\ \mathbf{Exp}} \quad \text{where } \forall v \in \mathsf{FV}(E).\ \Delta\ v\ \mathbf{self} > 0$$

$$\overline{\Delta|\Upsilon \vdash P\ \mathbf{Assert}} \quad \text{where } \forall v \in \mathsf{FV}(P).\ \Delta\ v\ \mathbf{self} > 0$$

$$\overline{\Delta|\Upsilon \vdash P\ \mathbf{Valid}} \quad \begin{array}{l}\text{where } \forall v \in \mathsf{FV}(P).\ \Delta\ v\ \mathbf{self} > 0 \\ \text{and } P \text{ is a valid assertion.}\end{array}$$

are satisfied. If and only if these conditions are satisfied, the write-proof that extends P^0 with $\langle \Delta_n^{\mathsf{max}} \rangle$ will be a proof.

Moreover, suppose there is some proof that extends P^0 with $\langle \Delta_n \rangle$ and that $\Delta_{\mathsf{root}} \leq \Delta_{\mathsf{root}}^{\mathsf{max}}$. Then by (6), $\Delta_n \leq \Delta_n^{\mathsf{max}}$ for all nodes n. It follows that, since the side conditions at passive n are met by Δ_n, they will be met by Δ_n^{max}, so that the write-proof that extends P^0 with Δ_n^{max} will also be a proof.

It follows that either the algorithm will find a proof that extends P^0 with $\Delta_{\mathsf{root}}^{\mathsf{max}}$ at the root, or there is no proof that extends P^0 with any $\Delta_{\mathsf{root}} \leq \Delta_{\mathsf{root}}^{\mathsf{max}}$.

The Finale (continued)

It follows that either the algorithm will find a proof that extends P^0 with $\Delta_{\text{root}}^{\text{max}}$ at the root, or there is no proof that extends P^0 with any $\Delta_{\text{root}} \leq \Delta_{\text{root}}^{\text{max}}$.

Specified Root Context: If $\Delta_{\text{root}}^{\text{max}}$ is the specified root context, then either the algorithm will find a proof that extends P^0 with $\Delta_{\text{root}}^{\text{max}}$ at the root, or, since $\Delta_{\text{root}}^{\text{max}} \leq \Delta_{\text{root}}^{\text{max}}$, there is no proof that extends P^0 with $\Delta_{\text{root}}^{\text{max}}$ at the root.

Arbitrary Root Context: Here $\Delta_{\text{root}}^{\text{max}}$ is the most permissive context satisfying Φ_{root}. Either the algorithm will find a proof that extends P^0, or there is no proof that extends P^0 with any Δ_{root} that satisfies Φ_{root}. But by (2), there is no proof that extends P_0 with any Δ_{root} that does not satisfies Φ_{root}.

The Passive Rules

$$\frac{}{\Delta|\Upsilon \vdash E\ \mathbf{Exp}}\ \text{where } \forall v \in \mathsf{FV}(E).\ \Delta\ v\ \mathbf{self} > 0$$

$$\frac{}{\Delta|\Upsilon \vdash P\ \mathbf{Assert}}\ \text{where } \forall v \in \mathsf{FV}(P).\ \Delta\ v\ \mathbf{self} > 0$$

$$\frac{}{\Delta|\Upsilon \vdash P\ \mathbf{Valid}}\ \text{where } \forall v \in \mathsf{FV}(P).\ \Delta\ v\ \mathbf{self} > 0,$$

where $\mathsf{FV}(X)$ denotes the set of free variables of X.

Φ is the empty function.

Since there are no premisses, there are no Δ_i^{max} to be computed. But the side conditions must be checked to determine if a write-proof is a proof.

The Rule for (Assignable) Variables

$$\overline{\Delta|\Upsilon \vdash v\ \mathbf{Var}}\,,$$

where

$$\begin{aligned}\Delta\, v'\, o &= 0 \text{ when } v' \neq v \\ \Delta\, v\, o &= \mathbf{if}\ o = \mathbf{self}\ \mathbf{then}\ 1\ \mathbf{else}\ 0.\end{aligned}$$

$$\operatorname{dom}\Phi = \{v\} \qquad \Phi\, v = \{\mathbf{self}\}.$$

Since there are no premisses, there are no Δ_i^{max} to be computed. Moreover, it is clear that Δ^{max} will meet the side condition since Δ^{max} will satisfy Φ.

Sequential Composition (Many rules are similar.)

$$\frac{\Delta_1|\Upsilon \vdash \{P\}\ C\ \{Q\} \quad \Delta_2|\Upsilon \vdash \{Q\}\ C'\ \{R\}}{\Delta|\Upsilon \vdash \{P\}\ C\ ; C'\ \{R\},}$$

where

$$\Delta_1 = \Delta_2 = \Delta.$$

$$\mathrm{dom}\,\Phi = \mathrm{dom}\,\Phi_1 \cup \mathrm{dom}\,\Phi_2.$$

When $v \in \mathrm{dom}\,\Phi$:

$$o \in \Phi\, v \ \text{ iff } \begin{cases} (v \in \mathrm{dom}\,\Phi_1 \Rightarrow o \in \Phi_1\, v) \\ \qquad\qquad \wedge \\ (v \in \mathrm{dom}\,\Phi_2 \Rightarrow o \in \Phi_2\, v), \end{cases}$$

or equivalently

$$o \notin \Phi\, v \ \text{ iff } \begin{cases} (v \in \mathrm{dom}\,\Phi_1 \wedge o \notin \Phi_1\, v) \\ \qquad\qquad \vee \\ (v \in \mathrm{dom}\,\Phi_2 \wedge o \notin \Phi_2\, v). \end{cases}$$

$$\Delta_1^{\mathrm{max}} = \Delta_2^{\mathrm{max}} = \Delta^{\mathrm{max}}.$$

Conditionals

$$\frac{\Delta_1|\Upsilon \vdash B\ \textbf{Assert} \qquad \Delta_2|\Upsilon \vdash \{P \wedge B\}\ C\ \{Q\} \quad \Delta_3|\Upsilon \vdash \{P \wedge \neg B\}\ C'\ \{Q\}}{\Delta|\Upsilon \vdash \{P\}\ \textbf{if}\ B\ \textbf{then}\ C\ \textbf{else}\ C'\ \{Q\},}$$

where

$$\Delta_1 = \Delta_2 = \Delta_3 = \Delta.$$

$$\mathsf{dom}\,\Phi = \mathsf{dom}\,\Phi_1 \cup \mathsf{dom}\,\Phi_2 \cup \mathsf{dom}\,\Phi_3.$$

When $v \in \mathsf{dom}\,\Phi$:

$$o \in \Phi\, v \ \text{ iff } \begin{cases} (v \in \mathsf{dom}\,\Phi_1 \Rightarrow o \in \Phi_1\, v) \\ \qquad\qquad\qquad \wedge \\ (v \in \mathsf{dom}\,\Phi_2 \Rightarrow o \in \Phi_2\, v) \\ \qquad\qquad\qquad \wedge \\ (v \in \mathsf{dom}\,\Phi_3 \Rightarrow o \in \Phi_3\, v). \end{cases}$$

$$\Delta_1^{\mathsf{max}} = \Delta_2^{\mathsf{max}} = \Delta_3^{\mathsf{max}} = \Delta^{\mathsf{max}}.$$

Note that Φ_1 will be the empty function.

Parallel Composition (Frame is similar)

$$\frac{\Delta_1|\Upsilon \vdash \{P\}\; C\; \{Q\} \quad \Delta_2|\Upsilon \vdash \{P'\}\; C'\; \{Q'\}}{\Delta|\Upsilon \vdash \{P \ast P'\}\; C \parallel C'\; \{Q \ast Q'\},}$$

where

$$\begin{array}{r}\Delta\, v\, o = \Delta_1\, v\, o = \Delta_2\, v\, o \text{ when } o \neq \mathbf{self} \\ \Delta\, v\, \mathbf{self} = \Delta_1\, v\, \mathbf{self} + \Delta_2\, v\, \mathbf{self} \leq 1.\end{array} \qquad \text{(A)}$$

$$\mathrm{dom}\,\Phi = \mathrm{dom}\,\Phi_1 \cup \mathrm{dom}\,\Phi_2.$$

When $v \in \mathrm{dom}\,\Phi$:

$$o \in \Phi\, v \text{ iff } \left\{ \begin{array}{c} (v \in \mathrm{dom}\,\Phi_1 \Rightarrow o \in \Phi_1\, v) \\ \wedge \\ (v \in \mathrm{dom}\,\Phi_2 \Rightarrow o \in \Phi_2\, v) \\ \wedge \\ (v \in \mathrm{dom}\,\Phi_1 \cap \mathrm{dom}\,\Phi_2 \Rightarrow o \neq \mathbf{self}), \end{array} \right.$$

or equivalently,

$$o \notin \Phi\, v \text{ iff } \left\{ \begin{array}{c} (v \in \mathrm{dom}\,\Phi_1 \wedge o \notin \Phi_1\, v) \\ \vee \\ (v \in \mathrm{dom}\,\Phi_2 \wedge o \notin \Phi_2\, v) \\ \vee \\ (v \in \mathrm{dom}\,\Phi_1 \cap \mathrm{dom}\,\Phi_2 \wedge o = \mathbf{self}). \end{array} \right. \qquad \text{(B)}$$

Parallel Composition (continued)

$$\left.\begin{array}{r}\Delta_1^{\mathsf{max}}\, v\, o = \Delta^{\mathsf{max}}\, v\, o \\ \Delta_2^{\mathsf{max}}\, v\, o = \Delta^{\mathsf{max}}\, v\, o\end{array}\right\} \text{ when } \; o \neq \mathbf{self}$$

$$\left.\begin{array}{l}\Delta_1^{\mathsf{max}}\, v\, \mathbf{self} = \Delta^{\mathsf{max}}\, v\, \mathbf{self} \\ \Delta_2^{\mathsf{max}}\, v\, \mathbf{self} = 0\end{array}\right\} \text{ when } \left\{\begin{array}{l} v \in \mathsf{dom}\, \Phi_1 \wedge \\ v \notin \mathsf{dom}\, \Phi_2\end{array}\right.$$

$$\left.\begin{array}{l}\Delta_1^{\mathsf{max}}\, v\, \mathbf{self} = 0 \\ \Delta_2^{\mathsf{max}}\, v\, \mathbf{self} = \Delta^{\mathsf{max}}\, v\, \mathbf{self}\end{array}\right\} \text{ when } \left\{\begin{array}{l} v \notin \mathsf{dom}\, \Phi_1 \wedge \\ v \in \mathsf{dom}\, \Phi_2\end{array}\right. \quad \text{(C)}$$

$$\left.\begin{array}{l}\Delta_1^{\mathsf{max}}\, v\, \mathbf{self} = \frac{1}{2}\Delta^{\mathsf{max}}\, v\, \mathbf{self} \\ \Delta_2^{\mathsf{max}}\, v\, \mathbf{self} = \frac{1}{2}\Delta^{\mathsf{max}}\, v\, \mathbf{self}\end{array}\right\} \text{ when } \left\{\begin{array}{l} v \in \mathsf{dom}\, \Phi_1 \wedge \\ v \in \mathsf{dom}\, \Phi_2\end{array}\right.$$

$$\left.\begin{array}{l}\Delta_1^{\mathsf{max}}\, v\, \mathbf{self} = \frac{1}{2}\Delta^{\mathsf{max}}\, v\, \mathbf{self} \\ \Delta_2^{\mathsf{max}}\, v\, \mathbf{self} = \frac{1}{2}\Delta^{\mathsf{max}}\, v\, \mathbf{self}\end{array}\right\} \text{ when } \left\{\begin{array}{l} v \notin \mathsf{dom}\, \Phi_1 \wedge \\ v \notin \mathsf{dom}\, \Phi_2\end{array}\right.$$

Parallel Composition — Proof of (1)

(1) If Δ_1 satisfies Φ_1, Δ_2 satisfies Φ_2, and (A) and (B), then Δ satisfies Φ.

Proof Suppose, for $i \in \{1, 2\}$, Δ_i satisfies Φ_i, so that

$\forall v \in \mathsf{dom}\,\Phi_i.\ \sum_{o \in \mathsf{Owners}} \Delta_i\, v\, o = 1$

$\forall v \in \mathsf{dom}\,\Phi_i, o \in \mathsf{Owners}.\ o \notin \Phi_i\, v$ implies $\Delta_i\, v\, o = 0$.

Now suppose $v \in \mathsf{dom}\,\Phi = \mathsf{dom}\,\Phi_1 \cup \mathsf{dom}\,\Phi_2$. If $v \in \mathsf{dom}\,\Phi_1$, then by (A):

$$\begin{aligned}\textstyle\sum_{o \in \mathsf{Owners}} \Delta\, v\, o &= (\textstyle\sum_{o \in \mathsf{Owners}} \Delta_1\, v\, o) + \Delta_2\, v\, \mathbf{self} \\ &= 1 + \Delta_2\, v\, \mathbf{self}.\end{aligned}$$

But $\sum_{o \in \mathsf{Owners}} \Delta\, v\, o \leq 1$, so

$$\textstyle\sum_{o \in \mathsf{Owners}} \Delta\, v\, o = 1 \quad \text{and} \quad \Delta_2\, v\, \mathbf{self} = 0.$$

Similarly, if $v \in \mathsf{dom}\,\Phi_2$, then

$$\textstyle\sum_{o \in \mathsf{Owners}} \Delta\, v\, o = 1 \quad \text{and} \quad \Delta_1\, v\, \mathbf{self} = 0.$$

Suppose $v \in \mathsf{dom}\,\Phi$ and $o \notin \Phi\, v$. Then, by (B), there are three possibilities, each of which implies $\Delta\, v\, o = 0$:

- $v \in \mathsf{dom}\,\Phi_1$ and $o \notin \Phi_1, v$, so that $\Delta_1\, v\, o = 0$ and $\Delta_2\, v\, \mathbf{self} = 0$.
- $v \in \mathsf{dom}\,\Phi_2$ and $o \notin \Phi_2, v$, so that $\Delta_2\, v\, o = 0$ and $\Delta_1\, v\, \mathbf{self} = 0$.
- $v \in \mathsf{dom}\,\Phi_1$, $v \in \mathsf{dom}\,\Phi_2$ and $o = \mathbf{self}$, so that $\Delta_2\, v\, \mathbf{self} = 0$, $\Delta_1\, v\, \mathbf{self} = 0$, and $o = \mathbf{self}$.

Thus we have

$\forall v \in \mathsf{dom}\,\Phi.\ \sum_{o \in \mathsf{Owners}} \Delta\, v\, o = 1$

$\forall v \in \mathsf{dom}\,\Phi, o \in \mathsf{Owners}.\ o \notin \Phi\, v$ implies $\Delta_i\, v\, o = 0$,

so that Δ satisfies Φ.

Parallel Composition — Proof of (3)

(3) If Δ^{max} satisfies Φ, then Δ_1^{max} and Δ_2^{max}, as defined by (C), satisfy Φ_1 and Φ_2 respectively, and

$$\begin{aligned} \Delta^{\mathsf{max}}\, v\, o = \Delta_1^{\mathsf{max}}\, v\, o = \Delta_2^{\mathsf{max}}\, v\, o \text{ when } o \neq \mathbf{self} \\ \Delta^{\mathsf{max}}\, v\, \mathbf{self} = \Delta_1^{\mathsf{max}}\, v\, \mathbf{self} + \Delta_2^{\mathsf{max}}\, v\, \mathbf{self} \leq 1. \end{aligned} \qquad \text{(D)}$$

Proof

It is easily seen that (C) satisfies (D).

To show that $\forall v \in \mathrm{dom}\,\Phi_1.\ \sum_{o \in \mathsf{Owners}}.\ \Delta_1^{\mathsf{max}}\, v\, o$, assume $v \in \mathrm{dom}\,\Phi_1$. From (D) we have

$$\textstyle\sum_{o \in \mathsf{Owners}} \Delta_1^{\mathsf{max}}\, v\, o = (\sum_{o \in \mathsf{Owners}} \Delta^{\mathsf{max}}\, v\, o) - \Delta_2^{\mathsf{max}}\, v\, \mathbf{self}.$$

When $v \notin \mathrm{dom}\,\Phi_2$, (C) gives $\Delta_2^{\mathsf{max}}\, v\, \mathbf{self} = 0$ directly. When $v \in \mathrm{dom}\,\Phi_2$, (B) gives $\mathbf{self} \notin \Phi\, v$ and since Δ^{max} is assumed to satisfy Φ, $\Delta^{\mathsf{max}}\, v\, \mathbf{self} = 0$, so that the penultimate case of (C) gives $\Delta_2^{\mathsf{max}}\, v\, \mathbf{self} = 0$. Thus, in either case,

$$\textstyle\sum_{o \in \mathsf{Owners}} \Delta_1^{\mathsf{max}}\, v\, o = \sum_{o \in \mathsf{Owners}} \Delta^{\mathsf{max}}\, v\, o = 1.$$

To show that

$\forall v \in \mathsf{dom}\,\Phi_1, o \in \mathsf{Owners}.\, o \notin \Phi_1\, v$ implies $\Delta_1^{\mathsf{max}}\, v\, o = 0$,

assume $v \in \mathsf{dom}\,\Phi_1$, $o \in \mathsf{Owners}$ and $o \notin \Phi_1\, v$. Then (B) gives $o \notin \Phi\, v$, and the the assumption that Δ^{max} satisfies Φ gives $\Delta^{\mathsf{max}}\, v\, o = 0$. Finally, (D) gives $\Delta_1^{\mathsf{max}}\, v\, o = 0$.

Thus Δ_1^{max} satisfies Φ_1. The argument for Δ_2^{max} satisfies Φ_2 is symmetric.

Parallel Composition — Proof of (4)

If Δ_1, Δ_2, and Δ satisfy Φ_1, Φ_2, and Φ respectively, (A) holds, and $\Delta \leq \Delta^{\mathsf{max}}$, then $\Delta_1 \leq \Delta_1^{\mathsf{max}}$ and $\Delta_2 \leq \Delta_2^{\mathsf{max}}$.

Proof Assume the hypotheses of the lemma, and $\Delta_1\, v\, o > 0$. To show $\Delta_1^{\mathsf{max}}\, v\, o > 0$, we first note that (A) gives $\Delta_1\, v\, o \leq \Delta\, v\, o$, which, with $\Delta \leq \Delta^{\mathsf{max}}$, gives

$$\Delta_1\, v\, o > 0 \Rightarrow \Delta\, v\, o > 0 \Rightarrow \Delta^{\mathsf{max}}\, v\, o > 0.$$

So we need to show $\Delta^{\mathsf{max}}\, v\, o > 0 \Rightarrow \Delta_1^{\mathsf{max}}\, v\, o > 0$.

- When $o \neq \mathbf{self}$, (D) gives $\Delta_1^{\mathsf{max}}\, v\, o = \Delta^{\mathsf{max}}\, v\, o$.
- When $o = \mathbf{self}$, (A) gives $\Delta_1\, v\, \mathbf{self} \leq \Delta\, v\, \mathbf{self}$. When $v \notin \mathsf{dom}\, \Phi_1$ and $v \in \mathsf{dom}\, \Phi_2$, since Δ_2 satisfies Φ_2, (A) gives

  $$\begin{aligned}\textstyle\sum_{o \in \mathsf{Owners}} \Delta\, v\, o &= (\textstyle\sum_{o \in \mathsf{Owners}} \Delta_2\, v\, o) + \Delta_1\, v\, \mathbf{self} \\ &= 1 + \Delta_1\, v\, \mathbf{self}.\end{aligned}$$

  so that $\sum_{o \in \mathsf{Owners}} \Delta\, v\, o \leq 1$ gives $\Delta_1\, v\, \mathbf{self} = 0$, which contradicts $\Delta_1\, v\, o > 0$.

  Otherwise, (C) gives

  $$\Delta^{\mathsf{max}}\, v\, \mathbf{self} > 0 \Rightarrow \Delta_1^{\mathsf{max}}\, v\, \mathbf{self} > 0.$$

The argument for $\Delta_2 \leq \Delta_2^{\mathsf{max}}$ is symmetric.

Resource Declaration

$$\frac{\Delta_1|\Upsilon \vdash R\ \mathbf{Assert} \qquad \Delta_2|\Upsilon, r\colon R \vdash \{P\}\ C\ \{Q\}}{\Delta|\Upsilon \vdash \{P * R\}\ \mathbf{resource}\ r\ \mathbf{in}\ C\ \{Q * R\},}\ (R \text{ precise})$$

where

$$\begin{aligned} \Delta\, v\, o &= \Delta_2\, v\, o \text{ when } o \notin \{\mathbf{self}, r\} \\ \Delta\, v\, \mathbf{self} &= \Delta_2\, v\, \mathbf{self} + \Delta_2\, v\, r \leq 1 \\ \Delta_1\, v\, o &= 0 \text{ when } o \neq \mathbf{self} \\ \Delta_1\, v\, \mathbf{self} &= \Delta_2\, v\, r. \end{aligned}$$

$$\mathrm{dom}\,\Phi = \mathrm{dom}\,\Phi_2.$$

When $v \in \mathrm{dom}\,\Phi$:

$$\begin{aligned} o \in \Phi\, v &\text{ iff } o \in \Phi_2\, v \text{ when } o \notin \{\mathbf{self}, r\} \\ r \notin \Phi\, v & \\ \mathbf{self} \in \Phi\, v &\text{ iff } \mathbf{self} \in \Phi_2\, v \vee r \in \Phi_2\, v. \end{aligned}$$

Resource Declaration (continued)

$$\Delta_2^{\mathsf{max}}\, v\, o = \Delta^{\mathsf{max}}\, v\, o \quad \text{when} \quad o \notin \{\mathbf{self}, r\}$$

$$\left.\begin{array}{r} \Delta_2^{\mathsf{max}}\, v\, \mathbf{self} = \frac{1}{2}\, \Delta^{\mathsf{max}}\, v\, \mathbf{self} \\ \Delta_2^{\mathsf{max}}\, v\, r = \frac{1}{2}\, \Delta^{\mathsf{max}}\, v\, \mathbf{self} \end{array}\right\} \quad \text{when} \quad v \notin \mathsf{dom}\, \Phi_2$$

$$\left.\begin{array}{r} \Delta_2^{\mathsf{max}}\, v\, \mathbf{self} = 0 \\ \Delta_2^{\mathsf{max}}\, v\, r = 0 \end{array}\right\} \quad \text{when} \quad \left\{\begin{array}{l} v \in \mathsf{dom}\, \Phi_2 \wedge \\ \mathbf{self} \notin \Phi_2\, v \wedge \\ r \notin \Phi_2\, v \end{array}\right.$$

$$\left.\begin{array}{l} \Delta_2^{\mathsf{max}}\, v\, \mathbf{self} = \Delta^{\mathsf{max}}\, v\, \mathbf{self} \\ \Delta_2^{\mathsf{max}}\, v\, r = 0 \end{array}\right\} \quad \text{when} \quad \left\{\begin{array}{l} v \in \mathsf{dom}\, \Phi_2 \wedge \\ \mathbf{self} \in \Phi_2\, v \wedge \\ r \notin \Phi_2\, v \end{array}\right.$$

$$\left.\begin{array}{l} \Delta_2^{\mathsf{max}}\, v\, \mathbf{self} = 0 \\ \Delta_2^{\mathsf{max}}\, v\, r = \Delta^{\mathsf{max}}\, v\, \mathbf{self} \end{array}\right\} \quad \text{when} \quad \left\{\begin{array}{l} v \in \mathsf{dom}\, \Phi_2 \wedge \\ \mathbf{self} \notin \Phi_2\, v \wedge \\ r \in \Phi_2\, v \end{array}\right.$$

$$\left.\begin{array}{r} \Delta_2^{\mathsf{max}}\, v\, \mathbf{self} = \frac{1}{2}\, \Delta^{\mathsf{max}}\, v\, \mathbf{self} \\ \Delta_2^{\mathsf{max}}\, v\, r = \frac{1}{2}\, \Delta^{\mathsf{max}}\, v\, \mathbf{self} \end{array}\right\} \quad \text{when} \quad \left\{\begin{array}{l} v \in \mathsf{dom}\, \Phi_2 \wedge \\ \mathbf{self} \in \Phi_2\, v \wedge \\ r \in \Phi_2\, v \end{array}\right.$$

$$\Delta_1^{\mathsf{max}}\, v\, o = 0 \quad \text{when} \quad o \neq \mathbf{self}$$

$$\Delta_1^{\mathsf{max}}\, v\, \mathbf{self} = \Delta_2^{\mathsf{max}}\, v\, r$$

Critical Regions

$$\frac{\begin{array}{cc}\Delta_1|\Upsilon, r\colon R \vdash P\ \mathbf{Assert} & \Delta_2|\Upsilon, r\colon R \vdash Q\ \mathbf{Assert} \\ \Delta_3|\Upsilon \vdash B\ \mathbf{Assert} & \Delta_4|\Upsilon \vdash \{(P * R) \wedge B\}\ C\ \{Q * R\}\end{array}}{\Delta|\Upsilon, r\colon R \vdash \{P\}\ \mathbf{with}\ r\ \mathbf{when}\ B\ \mathbf{do}\ C\ \{Q\},}$$

where

$$\Delta_1 = \Delta_2 = \Delta \qquad \Delta_3 = \Delta_4,$$

$$\begin{aligned} \Delta_4\, v\, o &= \Delta\, v\, o \text{ when } o \notin \{\mathbf{self}, r\} \\ \Delta_4\, v\, \mathbf{self} &= \Delta\, v\, \mathbf{self} + \Delta\, v\, r \leq 1 \\ \Delta_4\, v\, r &= 0. \end{aligned}$$

$$\mathrm{dom}\, \Phi = \mathrm{dom}\, \Phi_4.$$

When $v \in \mathrm{dom}\, \Phi$:

$$\begin{aligned} o \in \Phi\, v &\text{ iff } o \in \Phi_4\, v \text{ when } o \notin \{\mathbf{self}, r\} \\ \mathbf{self} \in \Phi\, v &\text{ iff } \mathbf{self} \in \Phi_4\, v \\ r \in \Phi\, v &\text{ iff } \mathbf{self} \in \Phi_4\, v. \end{aligned}$$

$$\Delta_1^{\mathsf{max}} = \Delta_2^{\mathsf{max}} = \Delta^{\mathsf{max}} \qquad \Delta_3^{\mathsf{max}} = \Delta_4^{\mathsf{max}},$$

$$\begin{aligned} \Delta_4^{\mathsf{max}}\, v\, o &= \Delta^{\mathsf{max}}\, v\, o \text{ when } o \notin \{\mathbf{self}, r\} \\ \Delta_4^{\mathsf{max}}\, v\, \mathbf{self} &= \Delta^{\mathsf{max}}\, v\, \mathbf{self} + \Delta^{\mathsf{max}}\, v\, r \\ \Delta_4^{\mathsf{max}}\, v\, r &= 0. \end{aligned}$$

Variable Declaration

$$\frac{\begin{array}{cc}\Delta_1|\Upsilon \vdash P \textbf{ Assert} & \Delta_2|\Upsilon \vdash Q \textbf{ Assert} \\ \Delta_3|\Upsilon \vdash E \textbf{ Exp} & \Delta_4|\Upsilon \vdash \{P\}\ C\ \{Q\}\end{array}}{\Delta|\Upsilon \vdash \{P\}\ \textbf{local}\ v := E\ \textbf{in}\ C\ \{Q\},}$$

where

$$\Delta_1 = \Delta_2 = \Delta_3 = \Delta,$$

$$\begin{array}{l}\Delta_4\, v'\, o = \Delta\, v'\, o \text{ when } v' \neq v \\ \Delta_4\, v\, o = \textbf{if } o = \textbf{self then } 1 \textbf{ else } 0.\end{array}$$

If $v \in \mathrm{dom}\,\Phi_4$ and $\textbf{self} \notin \Phi_4\, v$ then there is no write-proof extending P^0. Otherwise,

$$\mathrm{dom}\,\Phi = (\mathrm{dom}\,\Phi_4) - \{v\}$$

When $v' \in \mathrm{dom}\,\Phi$:

$$\Phi\, v' = \Phi_4\, v' \text{ when } v' \in \mathrm{dom}\,\Phi.$$

$$\Delta_1^{\max} = \Delta_2^{\max} = \Delta_3^{\max} = \Delta^{\max},$$

$$\begin{array}{l}\Delta_4^{\max}\, v'\, o = \Delta^{\max}\, v'\, o \text{ when } v' \neq v \\ \Delta_4^{\max}\, v\, o = \textbf{if } o = \textbf{self then } 1 \textbf{ else } 0.\end{array}$$