Class Notes for BRICS Minicourse - Fall 2003

SEPARATION LOGIC

7. Special Classes of Assertions

John C. Reynolds
Department of Computer Science
Carnegie Mellon University
and
BRICS
Aarhus University

Revised December 4, 2003

An Overview

- Pure
  - independent of the heap
- Intuitionistic
  - never falsified by extending the heap
- Strictly Exact
  - determines unique heap
- Domain-Exact
  - determines unique domain of heap
- Precise
  - For any heap, holds for at most one subset
- Supported
  - For any heap, if it holds for some subset, there is a least subset for which it holds.
- Universally Quantified Intuitionistic
  - $\forall x.\ x \hookrightarrow - \Rightarrow i(x)$.
- Immiscible
  - hold only for disjoint heaps

Pure Assertions

- An assertion is *pure* iff, for any store, it is independent of the heap.
- Syntactically, an assertion is pure if it does not contain **emp**, $\mapsto$, or $\hookrightarrow$.

$$
\begin{array}{cr}
p_1 \land p_2 \Rightarrow p_1 \ * \ p_2 & \text{when } p_1 \text{ or } p_2 \text{ is pure} \\
p_1 \ * \ p_2 \Rightarrow p_1 \land p_2 & \text{when } p_1 \text{ and } p_2 \text{ are pure} \\
(p \land q) \ * \ r \Leftrightarrow p \land (q \ * \ r) & \text{when } p \text{ is pure} \\
(p_1 \mathrel{-\!\!*} p_2) \Rightarrow (p_1 \Rightarrow p_2) & \text{when } p_1 \text{ is pure} \\
(p_1 \Rightarrow p_2) \Rightarrow (p_1 \mathrel{-\!\!*} p_2) & \text{when } p_1 \text{ and } p_2 \text{ are pure.}
\end{array}
$$

Intuitionistic Assertions

- An assertion i is *intuitionistic* iff, for all stores s and heaps h and h':

$$h \subseteq h' \text{ and } s, h \vDash i \text{ implies } s, h' \vDash i.$$

In the following, we assume i and i' are intuitionistic assertions, p is any assertion, and e and e' are expressions:

- Syntactically, the following assertions are intuitionistic:

$$\begin{array}{cc} \text{Any pure assertion} & p * i \\ p -\!\!* \; i & i -\!\!* \; p \\ i \wedge i' & i \vee i' \\ \forall v.\, i & \exists v.\, i, \end{array}$$

  and as special cases:

$$p * \textbf{true} \qquad \textbf{true} -\!\!* \; p \qquad e \hookrightarrow e'.$$

- The following laws hold:

$$i * p \Rightarrow i \qquad i \Rightarrow p -\!\!* \; i \qquad i * i' \Rightarrow i \wedge i'.$$

  (Note that $i * p \Rightarrow i$ is the weakening law.) Moreover, for arbitrary assertions,

$$p \Rightarrow p * \textbf{true} \qquad \textbf{true} -\!\!* \; p \Rightarrow p,$$

  so that

$$i * \textbf{true} \Leftrightarrow i \qquad i \Leftrightarrow \textbf{true} -\!\!* \; i.$$

Intuitionistic Assertions (continued)

- If $p \Rightarrow i$ then
$$p \ast \textbf{true} \Rightarrow i \ast \textbf{true},$$
and since $i \ast \textbf{true} \Leftrightarrow i$,
$$p \ast \textbf{true} \Rightarrow i.$$
Thus, since $p \Rightarrow p \ast \textbf{true}$, $p \ast \textbf{true}$ is the strongest intuitionistic assertion weaker than p.

- If $i \Rightarrow p$ then
$$\textbf{true} -\!\!\ast\, i \Rightarrow \textbf{true} -\!\!\ast\, p,$$
and since $i \Leftrightarrow \textbf{true} -\!\!\ast\, i$,
$$i \Rightarrow \textbf{true} -\!\!\ast\, p.$$
Thus, since $\textbf{true} -\!\!\ast\, p \Rightarrow p$, $\textbf{true} -\!\!\ast\, p$ is the weakest intuitionistic assertion stronger than p.

Intuitionistic Separation Logic

$$
\begin{aligned}
\langle\text{int assert}\rangle ::= \; & \langle\text{pure assert}\rangle \\
& \mid \; \overset{\mathrm{i}}{\neg}\, \langle\text{int assert}\rangle \\
& \mid \langle\text{int assert}\rangle \wedge \langle\text{int assert}\rangle \mid \langle\text{int assert}\rangle \vee \langle\text{int assert}\rangle \\
& \mid \langle\text{int assert}\rangle \overset{\mathrm{i}}{\Rightarrow} \langle\text{int assert}\rangle \mid \langle\text{int assert}\rangle \overset{\mathrm{i}}{\Leftrightarrow} \langle\text{int assert}\rangle \\
& \mid \forall\langle\text{var}\rangle.\ \langle\text{int assert}\rangle \mid \exists\langle\text{var}\rangle.\ \langle\text{int assert}\rangle \\
& \mid \langle\text{exp}\rangle \overset{\mathrm{i}}{\mapsto} \langle\text{exp}\rangle \\
& \mid \langle\text{int assert}\rangle \ast \langle\text{int assert}\rangle \\
& \mid \langle\text{int assert}\rangle \mathrel{-\!\!\ast} \langle\text{int assert}\rangle
\end{aligned}
$$

where

$$e \overset{\mathrm{i}}{\mapsto} e' \overset{\mathrm{def}}{=} e \hookrightarrow e' \overset{\mathrm{def}}{=} (e \mapsto e') \ast \mathbf{true}$$

$$\overset{\mathrm{i}}{\neg}\, p \overset{\mathrm{def}}{=} \mathbf{true} \mathrel{-\!\!\ast} (\neg\, p)$$

$$p \overset{\mathrm{i}}{\Rightarrow} q \overset{\mathrm{def}}{=} \mathbf{true} \mathrel{-\!\!\ast} (p \Rightarrow q)$$

$$p \overset{\mathrm{i}}{\Leftrightarrow} q \overset{\mathrm{def}}{=} \mathbf{true} \mathrel{-\!\!\ast} (p \Leftrightarrow q).$$

Strictly Exact Assertions (Yang)

- An assertion q is strictly exact iff, for all s, h, and h', $s, h \vDash q$ and $s, h' \vDash q$ implies $h = h'$.
- Syntactically, assertions built from expressions using **emp**, $\mapsto$, and $*$ are strictly exact.

Then:

$$((q \ * \ \mathbf{true}) \wedge p) \Rightarrow (q \ * \ (q \mathrel{-\!\!*} p)) \quad \text{when } q \text{ is strictly exact.}$$

For example,

$$(((e \mapsto e') \ * \ \mathbf{true}) \wedge p) \Rightarrow ((e \mapsto e') \ * \ ((e \mapsto e') \mathrel{-\!\!*} p)).$$

This is the fourth axiom schema for $\mapsto$, which is used to derive the backward-reasoning rule for lookup (LKBR) from the global rule (LKG).

Domain-Exact Assertions

- An assertion q is domain-exact iff, for all s, h, and h', $s, h \vDash q$ and $s, h' \vDash q$ implies $\mathrm{dom}\, h = \mathrm{dom}\, h'$.
- Strictly exact assertions are domain-exact.
- Syntactically, assertions built from expressions using **emp**, $\mapsto$, $-$, and $*$ are domain-exact.

Precise Assertions

- An assertion q is *precise* iff, for all s and h, there is at most one $h' \subseteq h$ such that $s, h' \vDash q$ is true.
- Domain-exact assertions are precise.
- Precise assertions include

$$\begin{array}{llll} \mathsf{list}\ \alpha\ \mathsf{i} & \mathsf{lseg}\ \alpha\ (\mathsf{i},\mathsf{j}) & \mathsf{ntlseg}\ \alpha\ (\mathsf{i},\mathsf{j}) & \mathsf{tree}\ \tau\ (\mathsf{i}) \\ \exists\alpha.\ \mathsf{list}\ \alpha\ \mathsf{i} & & \exists\alpha.\ \mathsf{ntlseg}\ \alpha\ (\mathsf{i},\mathsf{j}) & \exists\tau.\ \mathsf{tree}\ \tau\ (\mathsf{i}), \end{array}$$

  but not $\exists\alpha.\ \mathsf{lseg}\ \alpha\ (\mathsf{i},\mathsf{j})$.
- If p and q are precise, then $p * q$ is precise.
- If q is precise and $p \Rightarrow q$ is valid, then p is precise.
- Any assertion that is both intuitionistic and precise is unsatisfiable.
- When q is precise, the semidistributive laws given earlier become full distributive laws:

$$(p_1 * q) \wedge (p_2 * q) \Rightarrow (p_1 \wedge p_2) * q$$

  when q is precise

$$\forall x.\ (p * q) \Rightarrow (\forall x.\ p) * q$$

  when x not free in q, and q is precise.

Proof (of the first distributive law): Suppose $s, h \vDash (p_1 * q) \wedge (p_2 * q)$. Then there is an $h_1 \subseteq h$ such that $s, h - h_1 \vDash p_1$ and $s, h_1 \vDash q$, and there is an $h_2 \subseteq h$ such that $s, h - h_2 \vDash p_2$ and $s, h_2 \vDash q$. Then, since q is precise, $h_1 = h_2$, and $h - h_1 = h - h_2$, so that $s, h - h_1 \vDash p_1 \wedge p_2$, and $s, h \vDash (p_1 \wedge p_2) * q$.

Supported Assertions

- An assertion q is *supported* iff, for all s, h_1, and h_2,
  - if $h_1 \cup h_2$ is a function, and $s, h_1 \vDash q$ and $s, h_2 \vDash q$ are true,
  - then there is an h' such that $h' \subseteq h_1$, $h' \subseteq h_2$, and $s, h' \vDash q$ is true.
- An assertion q is *supported* iff, for all s and h, if the set

$$H = \{ h' \mid h' \subseteq h \text{ and } s, h' \vDash q \}$$

  is nonempty, then it has a least element.

Proof (that the first definition implies the second): Suppose that q satisfies the first definition, fix s and h, and let h_1 be a member of of H with minimum domain size, and h_2 be any member of H. Since h_1 and h_2 are both subsets of h, $h_1 \cup h_2$ must be a function. Then the first definition guarantees that there is an $h' \in H$ that is a subset of both h_1 and h_2. But h' must be equal to h_1, since otherwise it would have a smaller domain size. Thus $h_1 \subseteq h_2$ for every $h_2 \in H$.

Supported Assertions (continued)

- If q is precise, then q is supported.
- q is supported iff $q \,*\, \mathbf{true}$ is supported.

Proof: Suppose q is supported, $h_1 \cup h_2$ is a function, $s, h_1 \vDash q \,*\, \mathbf{true}$ and $s, h_2 \vDash q \,*\, \mathbf{true}$. Then there are $h'_1 \subseteq h_1$ and $h'_2 \subseteq h_2$ such that $s, h'_1 \vDash q$ and $s, h'_2 \vDash q$, and since q is supported, there is an h' that is a subset of h'_1 and h'_2, and therefore h_1 and h_2, such that $s, h' \vDash q$, and therefore $s, h' \vDash q \,*\, \mathbf{true}$.

Suppose $q \,*\, \mathbf{true}$ is supported, $h_1 \cup h_2$ is a function, $s, h_1 \vDash q$ and $s, h_2 \vDash q$. Then $s, h_1 \vDash q \,*\, \mathbf{true}$ and $s, h_2 \vDash q \,*\, \mathbf{true}$, and since $q \,*\, \mathbf{true}$ is supported, there is a common subset h' of h_1 and h_2 such that $s, h' \vDash q \,*\, \mathbf{true}$. But then there is a subset h'' of h', and therefore of h_1 and h_2, such that $s, h'' \vDash q$.

The analogous conjecture, that q is supported iff $\mathbf{true} \mathrel{-\!\!*} q$ is supported, fails in both directions. Suppose q is $1 \hookrightarrow 1 \vee 2 \hookrightarrow 2 \vee \mathbf{emp}$. Then q is supported, since the empty heap is the least heap in which it holds, but $\mathbf{true} \mathrel{-\!\!*} q$ is not supported, since it holds for the heaps $[\,1\colon 1\,]$ and $[\,2\colon 2\,]$, but not for their only common subheap, which is the empty heap.

On the other hand, suppose q is $1 \hookrightarrow 1 \vee 2 \mapsto 2$. Then $\mathbf{true} \mathrel{-\!\!*} q$ is supported, since $[\,1\colon 1\,]$ is the least heap for which it holds, but q is not supported, since it holds for $[\,1\colon 1\,]$ and $[\,2\colon 2\,]$, but not for the empty heap.

Supported Assertions (continued)

- When q is supported and the remaining assertions are intuitionistic, the semidistributive laws given earlier become full distributive laws:

$$(p_1 \ * \ q) \wedge (p_2 \ * \ q) \Rightarrow (p_1 \wedge p_2) \ * \ q$$

when p_1 and p_2 are intuitionistic and q is supported

$$\forall x.\ (p \ * \ q) \Rightarrow (\forall x.\ p) \ * \ q$$

when p is intuitionistic, q is supported, and x is not free in q.

Proof (of the first distributive law): Suppose $s, h \vDash (p_1 \ * \ q) \wedge (p_2 \ * \ q)$. Then there is an $h_1 \subseteq h$ such that $s, h - h_1 \vDash p_1$ and $s, h_1 \vDash q$, and there is an $h_2 \subseteq h$ such that $s, h - h_2 \vDash p_2$ and $s, h_2 \vDash q$. Then, since q is supported, and $h_1 \cup h_2$ is a subset of h (and therefore a function), there is a common subset h' of h_1 and h_2, and therefore of h, such that $s, h' \vDash q$. Then $h - h_1$ and $h - h_2$ are both subsets of $h - h'$, and since p_1 and p_2 are intuitionistic, $s, h - h' \vDash p_1$ and $s, h - h' \vDash p_2$. Therefore $s, h - h' \vDash (p_1 \wedge p_2)$, and $s, h \vDash (p_1 \wedge p_2) \ * \ q$.

The Precising Operation (Yang)

$$\mathrm{Pr}\, p \stackrel{\mathrm{def}}{=} p \wedge \neg(p \ast \neg\, \mathbf{emp}).$$

- If p is supported, then $\mathrm{Pr}\, p$ is precise.

Proof: Suppose p is supported, and $h_1, h_2 \subseteq h$ are such that $s, h_1 \vDash \mathrm{Pr}\, p$ and $s, h_2 \vDash \mathrm{Pr}\, p$.

We must show $h_1 = h_2$. Assume the contrary. Since $s, h_1 \vDash p$, $s, h_2 \vDash p$, and p is supported, there is a common subset h' of h_1 and h_2 such that $s, h' \vDash p$. Since $h_1 \neq h_2$, however, h' must be a proper subset of h_i for $i = 1$ or $i = 2$. Thus $h_i = h' \cdot (h_i - h')$, where $s, h_i - h' \vDash \neg\, \mathbf{emp}$. Then $s, h_i \vDash p \ast \neg\, \mathbf{emp}$, which contradicts $s, h_i \vDash \mathrm{Pr}\, p$.

- If p is precise, then $\mathrm{Pr}\, p \Leftrightarrow p$.

Proof: Obviously, $\mathrm{Pr}\, p \Rightarrow p$. To show the opposite implication when p is precise, assume $s, h \vDash p$. If $s, h \vDash p \ast \neg\, \mathbf{emp}$ held, then there would be a proper subset h' of h such that $s, h' \vDash p$, which would contradict the preciseness of p. Thus $s, h \vDash \neg(p \ast \neg\, \mathbf{emp})$.

The conjecture that, when p is supported, $\mathrm{Pr}\, p$ is the weakest precise assertion stronger than p, is false. Suppose p is the supported assertion $1 \mapsto 1 \vee \mathbf{emp}$. Then $1 \mapsto 1$ is a precise assertion stronger than p, but $\mathrm{Pr}\, p$, which is equivalent to $\mathbf{emp}$, is not weaker than $1 \mapsto 1$.

Precisification (continued)

- $\Pr\,(p \, * \, \mathbf{true}) \Rightarrow p$.

Proof: Suppose $s, h \vDash \Pr\,(p \, * \, \mathbf{true})$. Then $s, h \vDash p \, * \, \mathbf{true}$ and $s, h \vDash \neg(p \, * \, \mathbf{true} \, * \, \neg\,\mathbf{emp})$, and there is an $h' \subseteq h$ such that $s, h' \vDash p$. If $h' = h$, we are done; otherwise, h' is a proper subset of h, so that $s, h \vDash p \, * \, \mathbf{true} \, * \, \neg\,\mathbf{emp}$, which contradicts $s, h \vDash \neg(p \, * \, \mathbf{true} \, * \, \neg\,\mathbf{emp})$.

- $p \Rightarrow \Pr\,(p \, * \, \mathbf{true})$ when p is precise.

Proof: Suppose $s, h \vDash p$. Then $s, h \vDash p \, * \, \mathbf{true}$. Moreover, $s, h \vDash \neg(p \, * \, \mathbf{true} \, * \, \neg\,\mathbf{emp})$, for otherwise $s, h \vDash p \, * \, \mathbf{true} \, * \, \neg\,\mathbf{emp}$ would imply that there is a proper subset h' of h such that $s, h' \vDash p$, which would contradict the preciseness of p.

- $(\Pr\, q) \, * \, \mathbf{true} \Rightarrow q$ when q is intuitionistic.

Proof: Suppose $s, h \vDash (\Pr\, q) \, * \, \mathbf{true}$. Then there is an $h' \subseteq h$ such that $s, h' \vDash \Pr\, q$. Then $s, h' \vDash q$, and since q is intuitionistic, $s, h \vDash q$.

- $q \Rightarrow (\Pr\, q) \, * \, \mathbf{true}$ when q is supported.

Proof: Suppose $s, h \vDash q$. Since q is supported, there is a least $h' \subseteq h$ such that $s, h' \vDash q$. Then $s, h' \vDash \Pr\, q$, since otherwise $s, h' \vDash q \, * \, \neg\,\mathbf{emp}$, which would imply that a proper subset h'' of h' would satisfy $s, h'' \vDash q$, contradicting the leastness of h'. Thus $s, h \vDash (\Pr\, q) \, * \, \mathbf{true}$.

Universally Quantified Intuitionistic Assertions

Suppose i is intuitionistic, and let p be

$$\forall x.\ \mathsf{allocated}(x) \Rightarrow i,$$

where

$$\mathsf{allocated}(x) \equiv x \hookrightarrow -,$$

or, more generally,

$$s, h \vDash \mathsf{allocated}(x) \text{ iff } s\,x \in \mathrm{dom}\,h.$$

Then

$$\mathbf{emp} \Rightarrow p$$
$$(p \ * \ p) \Rightarrow p.$$

Immiscible Assertions

- Assertions p and q are *immiscible* iff, for all stores s and heaps h and h' such that $h \cup h'$ is a function, if $s, h \vDash p$ and $s, h' \vDash q$ then $h \perp h'$.

- If i and j are intuitionistic and $\neg(i \wedge j)$ is valid, then

  $$\forall x.\ \mathsf{allocated}(x) \Rightarrow i \qquad \text{and} \qquad \forall x.\ \mathsf{allocated}(x) \Rightarrow j$$

  are immiscible.

- If p' and q' are immiscible and $p \Rightarrow p'$ and $q \Rightarrow q'$ are valid, then p and q are immiscible.

If p and q are immiscible, then

$$(p \ast \mathbf{true}) \wedge (q \ast r) \Rightarrow q \ast ((p \ast \mathbf{true}) \wedge r)$$

is valid.

Relevance Conjunction (Bornat)

We define the logical operator $\bullet$ by:

$$s, h \vDash p_0 \bullet p_1 \text{ iff } \exists h_0, h_1.\ h_0 \cup h_1 = h \text{ and } s, h_0 \vDash p_0 \text{ and } s, h_1 \vDash p_1.$$

Note that h_0 and h_1 need not have disjoint domains.

Laws for Relevance Conjunction

$$\begin{aligned}
p &\Rightarrow p \bullet p \quad \text{(contraction)} \\
p * q &\Rightarrow p \bullet q \\
p \bullet q &\Rightarrow p * q \quad \text{when } p \text{ and } q \text{ are immiscible} \\
p \wedge q &\Rightarrow p \bullet q \\
i \bullet j &\Rightarrow i \wedge j \quad \text{when } i \text{ and } j \text{ are intuitionistic} \\
p_1 \bullet p_2 &\Leftrightarrow p_2 \bullet p_1 \\
(p_1 \bullet p_2) \bullet p_3 &\Leftrightarrow p_1 \bullet (p_2 \bullet p_3) \\
p \bullet \mathbf{emp} &\Leftrightarrow p \\
(p_1 \vee p_2) \bullet q &\Leftrightarrow (p_1 \bullet q) \vee (p_2 \bullet q) \\
(p_1 \wedge p_2) \bullet q &\Rightarrow (p_1 \bullet q) \wedge (p_2 \bullet q) \\
(\exists x.\ p_1) \bullet p_2 &\Leftrightarrow \exists x.\ (p_1 \bullet p_2) \quad \text{when } x \text{ not free in } p_2 \\
(\forall x.\ p_1) \bullet p_2 &\Rightarrow \forall x.\ (p_1 \bullet p_2) \quad \text{when } x \text{ not free in } p_2 \\
(p_1 \bullet p_2) * q &\Rightarrow (p_1 * q) \bullet (p_2 * q) \\
(p_1 * \mathbf{true}) \bullet (p_2 * \mathbf{true}) &\Rightarrow (p_1 \bullet p_2) * \mathbf{true}
\end{aligned}$$

$$\frac{p_1 \Rightarrow p_2 \qquad q_1 \Rightarrow q_2}{p_1 \bullet q_1 \Rightarrow p_2 \bullet q_2} \quad \text{(monotonicity)}$$

Also, if p and q are precise, then $p \bullet q$ is precise.

Precise Dags

For $\tau \in$ S-exps, we define

$$\mathsf{pdag}\,\tau\,(i)$$

by:

$$\mathsf{pdag}\,a\,(i) \text{ iff } \mathbf{emp} \wedge i = a$$

$$\begin{aligned}&\mathsf{pdag}\,(\tau_1 \cdot \tau_2)\,(i) \text{ iff}\\ &\qquad \exists i_1, i_2.\ i \mapsto i_1, i_2 \ * \ (\mathsf{pdag}\,\tau_1\,(i_1) \bullet \mathsf{pdag}\,\tau_2\,(i_2))\end{aligned}$$

It can be proved by induction on τ that $\mathsf{pdag}\,\tau\,(i)$ is precise.

Moreover,

$$\mathsf{pdag}\,\tau\,(i) \ * \ \mathbf{true} \Leftrightarrow \mathsf{dag}\,\tau\,(i).$$

This proof is also by induction on τ. In the base case

$$\begin{aligned}\mathsf{pdag}\,a\,(i) \ * \ \mathbf{true} &\Leftrightarrow (\mathbf{emp} \wedge i = a) \ * \ \mathbf{true}\\ &\Leftrightarrow i = a\\ &\Leftrightarrow \mathsf{dag}\,a\,(i).\end{aligned}$$

Precise Dags (continued)

The induction step is

$$
\begin{aligned}
&\mathsf{pdag}\,(\tau_1 \cdot \tau_2)\,(i) \;*\; \mathbf{true} \\
&\quad\Leftrightarrow (\exists i_1, i_2.\;\; i \mapsto i_1, i_2 \;*\; (\mathsf{pdag}\,\tau_1\,(i_1) \;\bullet\; \mathsf{pdag}\,\tau_2\,(i_2))) \;*\; \mathbf{true} \\
&\quad\Leftrightarrow \exists i_1, i_2.\;\; i \mapsto i_1, i_2 \;*\; (\mathsf{pdag}\,\tau_1\,(i_1) \;\bullet\; \mathsf{pdag}\,\tau_2\,(i_2)) \;*\; \mathbf{true} \\
&\quad\Leftrightarrow \exists i_1, i_2.\;\; i \mapsto i_1, i_2 \;* \\
&\qquad\quad ((\mathsf{pdag}\,\tau_1\,(i_1) \;*\; \mathbf{true}) \;\bullet\; (\mathsf{pdag}\,\tau_2\,(i_2) \;*\; \mathbf{true})) \\
&\quad\Leftrightarrow \exists i_1, i_2.\;\; i \mapsto i_1, i_2 \;*\; (\mathsf{dag}\,\tau_1\,(i_1) \;\bullet\; \mathsf{dag}\,\tau_2\,(i_2)) \\
&\quad\Leftrightarrow \exists i_1, i_2.\;\; i \mapsto i_1, i_2 \;*\; (\mathsf{dag}\,\tau_1\,(i_1) \wedge \mathsf{dag}\,\tau_2\,(i_2)) \\
&\quad\Leftrightarrow \mathsf{dag}\,\tau\,(i).
\end{aligned}
$$

From this result, we can also obtain

$$\mathsf{pdag}\,\tau\,(i) \Leftrightarrow \mathrm{Pr}\,(\mathsf{dag}\,\tau\,(i)).$$

Moreover, since $\mathsf{pdag}\,\tau(\mathsf{i}) \Rightarrow \mathsf{dag}\,\tau(\mathsf{i})$, we have the following specification of $\mathsf{copytree}$:

$$
\begin{aligned}
&\{\mathsf{p} \wedge \mathsf{pdag}\,\tau(\mathsf{i})\} \\
&\{\mathsf{p} \wedge \mathsf{dag}\,\tau(\mathsf{i})\} \\
&\mathsf{copytree}(\mathsf{i};\mathsf{j}) \\
&\{\mathsf{p} \;*\; \mathsf{tree}\,\tau(\mathsf{j})\}.
\end{aligned}
$$

Parameterless Proper Procedures (with free variables)

Let $k_1, \ldots, k_n$ be identifiers that stand for commands. We introduce judgements containing hypotheses about these identifiers:

$$\{p_1\}\ k_1\ \{q_1\}, \ldots, \{p_n\}\ k_n\ \{q_n\} \vdash \{p\}\ c\ \{q\}.$$

Then

$$\frac{}{\Gamma, \{p_i\}\ k_i\ \{q_i\}, \Gamma' \vdash \{p_i\}\ k_i\ \{q_i\}},$$

and

$$\frac{\Gamma, \{p_n\}\ k_n\ \{q_n\} \vdash \{p\}\ c\ \{q\} \qquad \{p_n\}\ c_n\ \{q_n\}}{\Gamma \vdash \{p\}\ (c/k_n \to c_n)\ \{q\}},$$

or

$$\frac{\Gamma, \{p_n\}\ k_n\ \{q_n\} \vdash \{p\}\ c\ \{q\} \qquad \{p_n\}\ c_n\ \{q_n\}}{\Gamma \vdash \{p\}\ \mathbf{proc}\ k_n = c_n\ \mathbf{in}\ c\ \{q\}}.$$

The Hypothetical Frame Rule

Subject to certain conditions:

$$\frac{\{p_1\}\ k_1\ \{q_1\}, \ldots, \{p_n\}\ k_n\ \{q_n\} \vdash \{p\}\ c\ \{q\}}{\{p_1 * r\}\ k_1\ \{q_1 * r\}, \ldots, \{p_n * r\}\ k_n\ \{q_n * r\} \vdash \{p * r\}\ c\ \{q * r\}}$$

where c does not assign to any variable free in r.

An Example of the Hypothetical Frame Rule

Let

$$ALLOC \stackrel{\text{def}}{=} \textbf{if } \mathsf{f} = \textbf{nil} \textbf{ then } \mathsf{x} := \textbf{cons}(0, \textbf{nil}) \textbf{ else} \\ (\mathsf{x} := \mathsf{f} \,;\, \mathsf{f} := [\mathsf{x}+1])$$

$$FREE \stackrel{\text{def}}{=} ([\mathsf{x}+1] := \mathsf{f} \,;\, \mathsf{f} := \mathsf{x})$$

$$r \stackrel{\text{def}}{=} \exists \alpha.\ \mathsf{list}\ \alpha\ \mathsf{f},$$

so that

$$\{\textbf{emp} * r\}\ ALLOC\ \{\mathsf{x} \mapsto -,- * r\}$$

and

$$\{\mathsf{x} \mapsto -,- * r\}\ FREE\ \{\textbf{emp} * r\}.$$

Now suppose

$$\{\textbf{emp}\}\ \mathsf{alloc}\ \{\mathsf{x} \mapsto -,-\}, \{\mathsf{x} \mapsto -,-\}\ \mathsf{free}\ \{\textbf{emp}\} \vdash \{p\}\ c\ \{q\}.$$

Then the hypothetical frame rule gives

$$\{\textbf{emp} * r\}\ \mathsf{alloc}\ \{\mathsf{x} \mapsto -,- * r\}, \{\mathsf{x} \mapsto -,- * r\}\ \mathsf{free}\ \{\textbf{emp} * r\} \\ \vdash \{p * r\}\ c\ \{q * r\},$$

so that

$$\{p * r\}\ (c/\mathsf{alloc} \to ALLOC, \mathsf{free} \to FREE)\ \{q * r\},$$

or

$$\{p * r\}\ \textbf{proc}\ \mathsf{alloc} = ALLOC\ \textbf{in proc}\ \mathsf{free} = FREE\ \textbf{in}\ c\ \{q * r\}.$$

A Counterexample

Let

$$\mathbf{one} \stackrel{\mathrm{def}}{=} \exists \mathsf{x}.\ \mathsf{x} \mapsto -.$$

Then

$$\{\mathbf{emp} \vee \mathbf{one}\}\ \mathsf{k}\ \{\mathbf{emp}\} \vdash \{\mathbf{emp} \vee \mathbf{one}\}\ \mathsf{k}\ \{\mathbf{emp}\}$$

$$\{\mathbf{emp} \vee \mathbf{one}\}\ \mathsf{k}\ \{\mathbf{emp}\} \vdash \{\mathbf{emp}\}\ \mathsf{k}\ \{\mathbf{emp}\}$$

$$\{\mathbf{emp} \vee \mathbf{one}\}\ \mathsf{k}\ \{\mathbf{emp}\} \vdash \{\mathbf{emp} \ast \mathbf{one}\}\ \mathsf{k}\ \{\mathbf{emp} \ast \mathbf{one}\} \quad (1)$$

$$\{\mathbf{emp} \vee \mathbf{one}\}\ \mathsf{k}\ \{\mathbf{emp}\} \vdash \{\mathbf{one}\}\ \mathsf{k}\ \{\mathbf{one}\}$$

$$\{\mathbf{emp} \vee \mathbf{one}\}\ \mathsf{k}\ \{\mathbf{emp}\} \vdash \{\mathbf{one}\}\ \mathsf{k}\ \{\mathbf{emp}\}$$

$$\{\mathbf{emp} \vee \mathbf{one}\}\ \mathsf{k}\ \{\mathbf{emp}\} \vdash \{\mathbf{one}\}\ \mathsf{k}\ \{\mathbf{emp} \wedge \mathbf{one}\} \quad (2)$$

$$\{\mathbf{emp} \vee \mathbf{one}\}\ \mathsf{k}\ \{\mathbf{emp}\} \vdash \{\mathbf{one}\}\ \mathsf{k}\ \{\mathbf{false}\}$$

$$\{(\mathbf{emp} \vee \mathbf{one}) \ast \mathbf{true}\}\ \mathsf{k}\ \{\mathbf{emp} \ast \mathbf{true}\}$$
$$\vdash \{\mathbf{one} \ast \mathbf{true}\}\ \mathsf{k}\ \{\mathbf{false} \ast \mathbf{true}\} \quad (3)$$

$$\{\mathbf{true}\}\ \mathsf{k}\ \{\mathbf{true}\} \vdash \{\mathbf{one} \ast \mathbf{true}\}\ \mathsf{k}\ \{\mathbf{false}\}$$

$$\{\mathbf{true}\}\ \mathbf{skip}\ \{\mathbf{true}\}$$

$$\{\mathbf{one} \ast \mathbf{true}\}\ \mathbf{skip}\ \{\mathbf{false}\}$$

1. by frame rule
2. by conjunction rule
3. by hypothetical frame rule

A Solution

Let $k_1, \ldots, k_n$ be identifiers that stand for commands.

1. If either r or each of $p_1, \ldots, p_n$ are precise assertions,

2. or if all of the assertions are intuitionistic and r is a supported assertion,

Then

$$\frac{\{p_1\}\ k_1\ \{q_1\}, \ldots, \{p_n\}\ k_n\ \{q_n\} \vdash \{p\}\ c\ \{q\}}{\{p_1 * r\}\ k_1\ \{q_1 * r\}, \ldots, \{p_n * r\}\ k_n\ \{q_n * r\} \vdash \{p * r\}\ c\ \{q * r\}}$$

where c does not assign to any variable free in r.

A Recent Generalization

2. or if each of the $q_1, \ldots, q_n$ are intuitionistic assertions, and either r or each of $p_1, \ldots, p_n$ are supported assertions.

See P. W. O'Hearn, H.Yang, J. C. Reynolds, "Separation and Information Hiding", POPL '04.