Response Under Compassion

So far, we only considered proofs of response properties under the fairness requirements of justice. Consider now the more general case, where also compassion requirements are included. The following rule can be used to establish response properties for this general case:

Rule RESP

For a well-founded domain $(\mathcal{A}, \succ)$,
fair transitions $t_1, \ldots, t_m$,
assertions $p, q = h_0, h_1, \ldots, h_m$,
and ranking functions $\delta_1, \ldots, \delta_m : \Sigma \mapsto \mathcal{A}$

R1. $p \Rightarrow \bigvee_{j=0}^{m} h_j$

For $i = 1, \ldots, m$

R2. $h_i \wedge \rho_t \Rightarrow (h'_i \wedge \delta_i = \delta'_i) \vee \bigvee_{j=0}^{m} (h'_j \wedge \delta_i \succ \delta'_j)$ For every $t \neq t_i$

R3. $h_i \wedge \rho_{t_i} \Rightarrow \bigvee_{j=0}^{m} (h'_j \wedge \delta_i \succ \delta'_j)$

R4. $h_i \Rightarrow En(t_i)$ If t_i is a just transition

R5. $h_i \Rightarrow \Diamond\, En(t_i)$ If t_i is a compassionate transition

---

$p \Rightarrow \Diamond\, q$

Thus, while for a just transition t_i, h_i should imply that t_i is enabled now, in the compassionate case, h_i only implies that t_i will be eventually enabled.

Justification of the Rule

On the face of it, rule RESP may appear to be circular. In order to prove a response property it requires, as a premise, another response property.

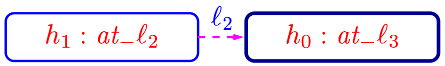
However, there is a certain reduction between the conclusion and the temporal premise. Namely, when establishing the eventual enableness of t_i we only consider computations which never activate t_i itself.

Example: MUX-SEM for 2 Processes

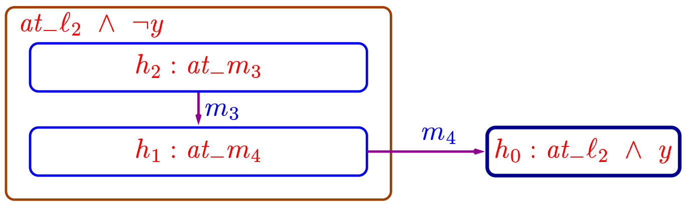
y: **natural initially** $y = 1$

$$P_1 :: \left[\begin{array}{l} \ell_0 : \textbf{loop forever do} \\ \left[\begin{array}{ll} \ell_1 : & \textbf{Non-critical} \\ \ell_2 : & \textbf{request } y \\ \ell_3 : & \textbf{Critical} \\ \ell_4 : & \textbf{release } y \end{array}\right] \end{array}\right] \parallel P_2 :: \left[\begin{array}{l} m_0 : \textbf{loop forever do} \\ \left[\begin{array}{ll} m_1 : & \textbf{Non-critical} \\ m_2 : & \textbf{request } y \\ m_3 : & \textbf{Critical} \\ m_4 : & \textbf{release } y \end{array}\right] \end{array}\right]$$

Following is a verification diagram for the property $at\_\ell_2 \Rightarrow \Diamond\, at\_\ell_3$:

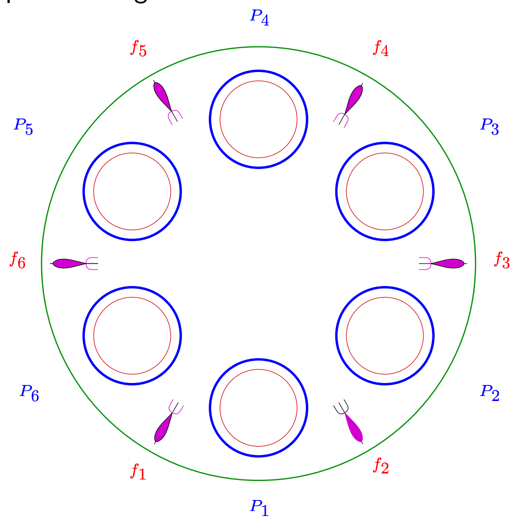


All the verification conditions generated by this verification diagram are non-temporal, except for the instance of premise R5 for transition ℓ_2 which has the form $at\_\ell_2 \Rightarrow \Diamond\, (at\_\ell_2 \wedge y)$. Using the auxiliary invariant $at\_\ell_{3,4} + at\_m_{3,4} + y = 1$, the required temporal property can be established by the following verification diagram:



The Dining Philosophers Metaphor

Consider n philosophers arranged around a table.



The life of a philosopher alternates between a thinking phase (a non-critical activity) and an eating phase. In order to eat, a philosopher needs both forks.

Program Dine

A first attempt yields the following program Dine:

in n : **integer initially** $n \geq 2$
local f : **array** $[1..n]$ **of integer initially** $f = 1$

$$\overset{n}{\underset{j=1}{\|}} P[j] :: \left[\begin{array}{l} \ell_0 : \textbf{loop forever do} \\ \left[\begin{array}{ll} \ell_1 : & \textbf{Non-Critical} \\ \ell_2 : & \textbf{request } f[j] \\ \ell_3 : & \textbf{request } f[j \oplus_n 1] \\ \ell_4 : & \textbf{Critical} \\ \ell_5 : & \textbf{release } f[j] \\ \ell_6 : & \textbf{release } f[j \oplus_n 1] \end{array}\right] \end{array}\right]$$

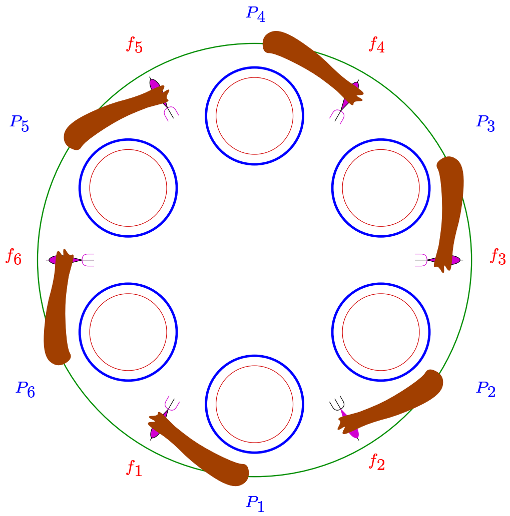
It is not difficult to verify the following safety property

$\square \neg(at\_\ell_4[1] \ \wedge \ at\_\ell_4[2]),$

stating that philosophers $P[1]$ and $P[2]$ can never eat at the same time.

Accessibility not Guaranteed

Unfortunately, Dine cannot ensure accessibility for $P[1]$, specifiable by
$\square \ (at\_\ell_2[1] \quad \rightarrow \quad \diamond \ at\_\ell_4[1])$
Because all philosophers may deadlock together.



Solution: One Contrary Philosopher

local f : **array** $[1..n]$ **of natural initially** $f = 1$

$\overset{n-1}{\underset{j=1}{\|}} P[j]$ ::
- ℓ_0 : **loop forever do**
  - ℓ_1 : **Non-Critical**
  - ℓ_2 : **request** $f[j]$
  - ℓ_3 : **request** $f[j{+}1]$
  - ℓ_4 : **Critical**
  - ℓ_5 : **release** $f[j]$
  - ℓ_6 : **release** $f[j{+}1]$

$\|$

$P[n]$ ::
- ℓ_0 : **loop forever do**
  - ℓ_1 : **Non-Critical**
  - ℓ_2 : **request** $f[1]$
  - ℓ_3 : **request** $f[n]$
  - ℓ_4 : **Critical**
  - ℓ_5 : **release** $f[1]$
  - ℓ_6 : **release** $f[n]$

Wish to establish accessibility, expressible by

ψacc: $\square\ (at\_\ell_2[j] \ \rightarrow\ \diamond\ (at\_\ell_4[j]))$

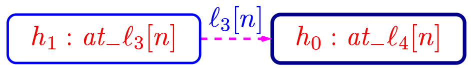
Prove A Chain of Eventualities

Before proving accessibility for arbitrary j, we will establish

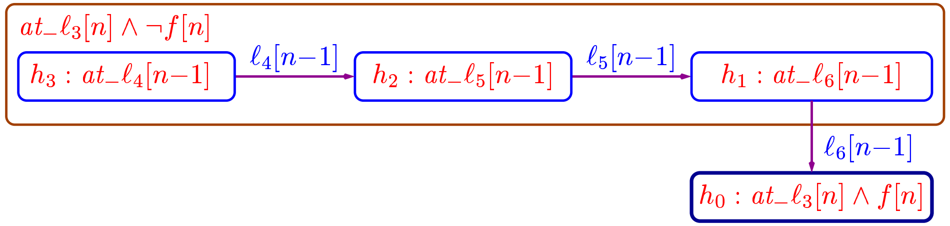
$$A_{3,4}[i] : at\_\ell_3[i] \quad \Rightarrow \quad \diamond\ at\_\ell_4[i]$$

by induction for $i = n, n-1, \ldots, 1$.

Induction Base: $A_{3,4}[n] : at\_\ell_3[n] \quad \Rightarrow \quad \diamond\ at\_\ell_4[n]$

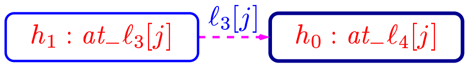


Premise R5 for $\ell_3[n]$ requires showing $at\_\ell_3[n] \Rightarrow \diamond\ (at\_\ell_3[n] \wedge f[n])$. Using the invariant $at\_\ell_{4..6}[n] + at\_\ell_{4..6}[n{-}1] + f[n] = 1$, this can be established by the following verification diagram:



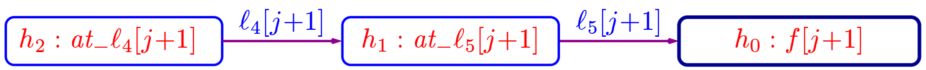
The Induction Step

We will now show that, assuming $A_{3,4}[j{+}1] : at\_\ell_3[j{+}1] \Rightarrow \Diamond\ at\_\ell_4[j{+}1]$, we can establish $A_{3,4}[j] : at\_\ell_3[j] \Rightarrow \Diamond\ at\_\ell_4[j]$, for every $j < n$. This is established by the following verification diagram:



Premise R5 for $\ell_3[j]$ requires showing $at\_\ell_3[j] \Rightarrow \Diamond\ (at\_\ell_3[j] \wedge f[j{+}1])$. Using the invariant $at\_\ell_{4..6}[j] + at\_\ell_{3..5}[j{+}1] + f[j{+}1] = 1$, we construct the following proof:

1.	$at\_\ell_3[j]$	$\Rightarrow$	$at\_\ell_3[j{+}1] \vee at\_\ell_{4,5}[j{+}1] \vee f[j{+}1]$	According to the invariant
2.	$at\_\ell_3[j{+}1]$	$\Rightarrow$	$\Diamond\ at\_\ell_4[j{+}1]$	By induction hypothesis
3.	$at\_\ell_{4,5}[j{+}1]$	$\Rightarrow$	$\Diamond\ f[j{+}1]$	Verification diagram below
4.	$at\_\ell_3[j]$	$\Rightarrow$	$\Diamond\ f[j{+}1]$	Temporal reasoning on 1–3

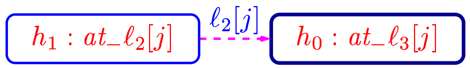


Verifying Accessibility

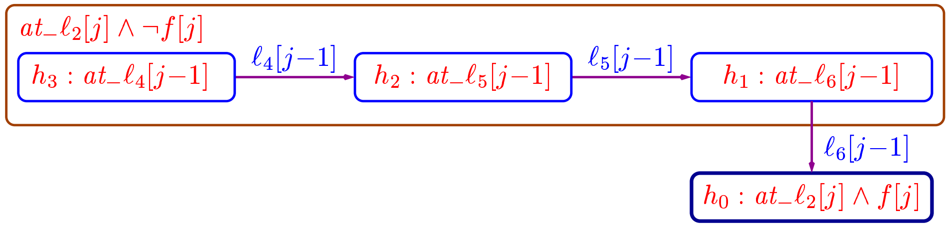
Finally, we verify $at\_\ell_2[j] \Rightarrow \Diamond\ at\_\ell_4[j]$, for all j, $1 < j < n$. The proof follows:

1.	$at\_\ell_2[j]$	$\Rightarrow$	$\Diamond\ at\_\ell_3[j]$	Verification diagram below
2.	$at\_\ell_3[j]$	$\Rightarrow$	$\Diamond\ at\_\ell_4[j]$	Proven by induction
3.	$at\_\ell_2[j]$	$\Rightarrow$	$\Diamond\ at\_\ell_4[j]$	Temporal reasoning on 1–2

The verification diagram for $at\_\ell_2[j] \Rightarrow \Diamond\ at\_\ell_3[j]$ is given by:



Premise R5 for $\ell_2[j]$ requires showing $at\_\ell_2[j] \Rightarrow \Diamond\ (at\_\ell_2[j] \wedge f[j])$. Using the invariant $at\_\ell_{3..5}[j] + at\_\ell_{4..6}[j{-}1] + f[j] = 1$, this can be established by the following verification diagram:



A Distributed Rank Justice-Base Rule

In some cases there is no 1–1 correspondence between justice requirements and transitions. In this case, we have to go back to a rule which is based on justice requirements rather than on transitions.

Rule DISTR-JUST
For a well-founded domain $(\mathcal{A}, \succ)$
For justice requirements $J_1, \ldots, J_m$,
assertions $p, q = h_0, h_1, \ldots, h_m$,
and ranking functions $\delta_1, \ldots, \delta_m : \Sigma \mapsto \mathcal{A}$

D1. $p \Rightarrow \bigvee_{j=0}^{m} h_j$

For $i = 1, \ldots, m$

D2. $h_i \wedge \rho \Rightarrow h_i' \vee \left((\bigvee_{j=0}^{m} h_j') \wedge (\bigvee_{j=1}^{m} (\delta_j \succ \delta_j')) \right)$

D3. $h_i \wedge \rho \Rightarrow \bigwedge_{j=1}^{m} (\delta_j \succeq \delta_j')$

D4. $h_i \Rightarrow \neg J_i$

$p \Rightarrow \diamondsuit\, q$

Reducing Compassion to Justice

An alternative approach to the verification of reponse properties over systems with compassion requirements is based on the reduction of compassion into justice.

Let $\mathcal{D} : \langle V, \Theta, \rho, \mathcal{J}, \mathcal{C} \rangle$ be an FDS with a non=empty set of compassion requirements. We construct a system $\mathcal{D}_{\mathcal{J}} : \langle V_{\mathcal{J}}, \Theta_{\mathcal{J}}, \rho_{\mathcal{J}}, \mathcal{J}_{\mathcal{J}}, \emptyset \rangle$ which contains no compassion requirements. Its constituents are give by:

$$V_{\mathcal{J}} : \quad V \cup \{nevermore_i : \textbf{boolean} \mid (p_i, q_i) \in \mathcal{C}\}$$
$$\Theta_{\mathcal{J}} : \quad \Theta \wedge \bigwedge_{(p_i,q_i)\in\mathcal{C}} \neg nevermore_i$$
$$\rho_{\mathcal{J}} : \quad \rho \vee \bigvee_{(p_i,q_i)\in\mathcal{C}} (nevermore_i := 1)$$
$$\mathcal{J}_{\mathcal{J}} : \quad \mathcal{J} \cup \{nevermore_i \vee q_i \mid (p_i, q_i) \in \mathcal{C}\}$$
$$\mathcal{C}_{\mathcal{J}} : \quad \emptyset$$

Then, we can use the following reduction:

In order to prove $\mathcal{D} \models \varphi \Rightarrow \diamondsuit\, \psi$, it is sufficient to prove
$\mathcal{D}_{\mathcal{J}} \models \varphi \Rightarrow \diamondsuit\, (\psi \vee \bigvee_{(p_i,q_i)\in\mathcal{C}} (p_i \wedge nevermore_i))$.