

## 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  $t_1, \dots, t_m$ ,

assertions  $p, q = h_0, h_1, \dots, h_m$ ,

and ranking functions  $\delta_1, \dots, \delta_m : \Sigma \mapsto \mathcal{A}$

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

For  $i = 1, \dots, m$

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

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

$$\text{R4. } h_i \Rightarrow \text{En}(t_i) \quad \text{If } t_i \text{ is a just transition}$$

$$\text{R5. } h_i \Rightarrow \diamond \text{En}(t_i) \quad \text{If } t_i \text{ is a compassionate transition}$$

---


$$p \Rightarrow \diamond q$$

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.

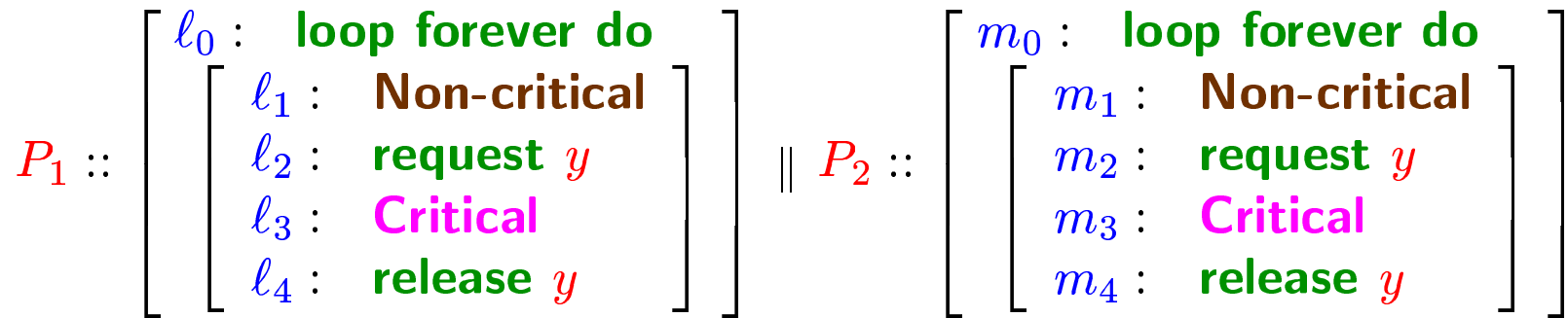
## Justification of the Rule

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.

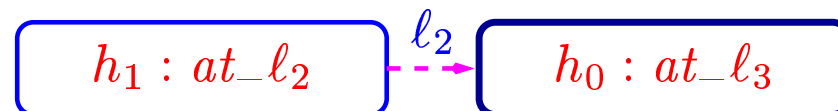
However, there is a certain reduction between the conclusion and the temporal premise. Namely, when establishing the eventual enableness of  $t_i$  we only consider computations which never activate  $t_i$  itself.

## Example: MUX-SEM for 2 Processes

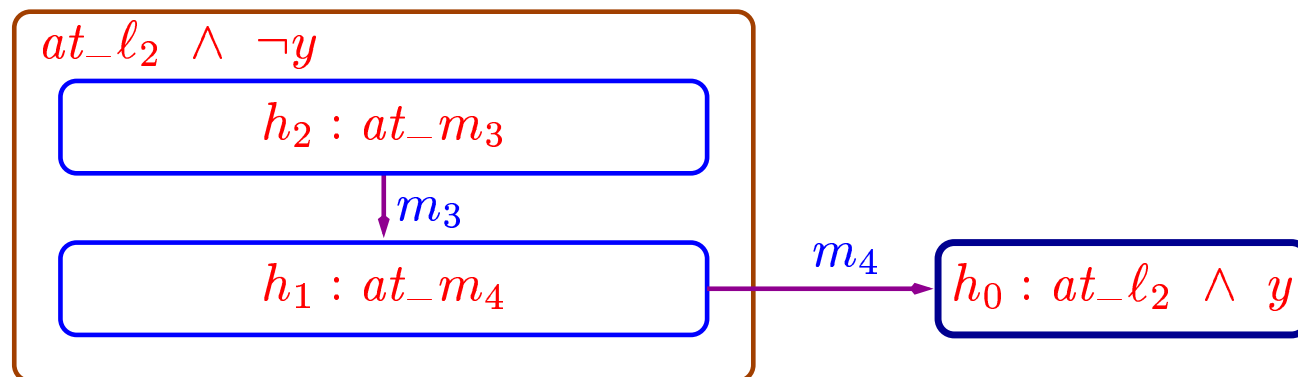
$y$ : natural initially  $y = 1$



Following is a verification diagram for the property  $at\_l_2 \Rightarrow \diamond at\_l_3$ :

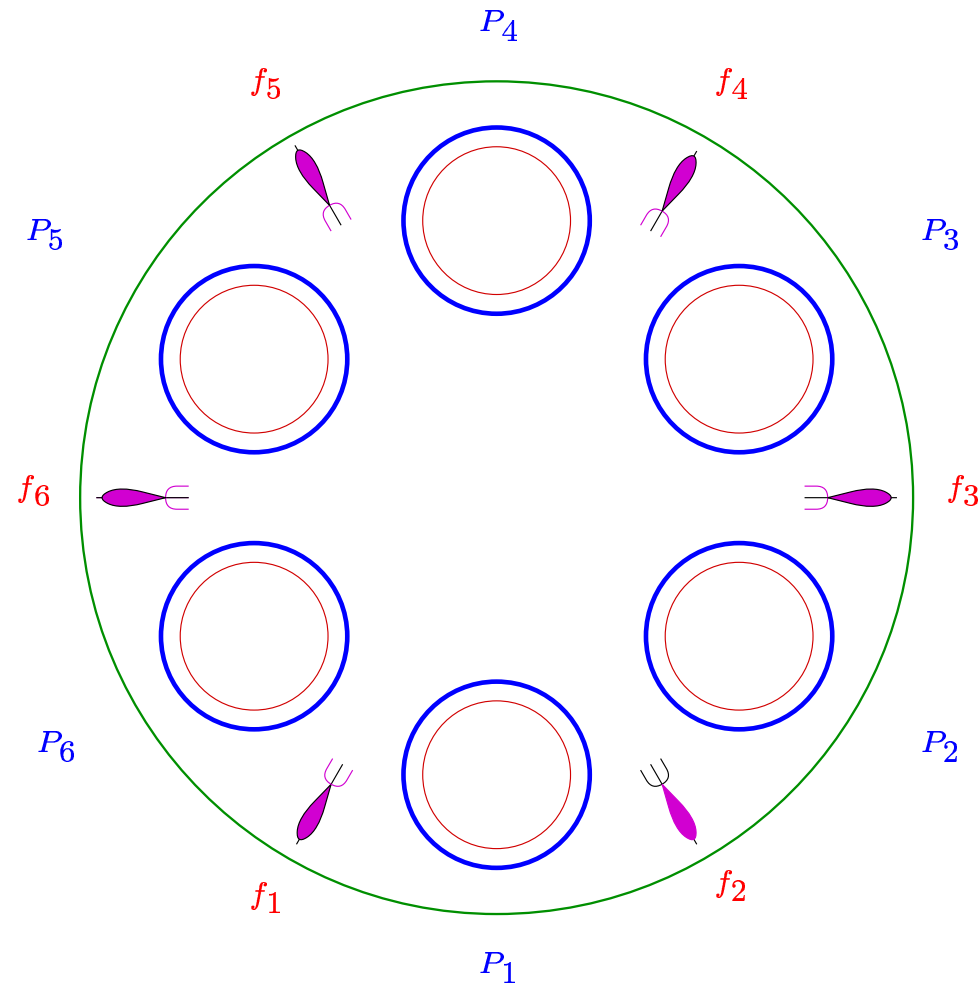


All the verification conditions generated by this verification diagram are non-temporal, except for the instance of premise R5 for transition  $l_2$  which has the form  $at\_l_2 \Rightarrow \diamond (at\_l_2 \wedge y)$ . Using the auxiliary invariant  $at\_l_{3,4} + at\_m_{3,4} + y = 1$ , the required 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**:

<b>in</b>	$n$	:	<b>integer initially</b>	$n \geq 2$
<b>local</b>	$f$	:	<b>array</b>	$[1..n]$ <b>of integer initially</b>
				$f = 1$
$\left[ \begin{array}{l} l_0 : \text{loop forever do} \\ \left[ \begin{array}{l} l_1 : \text{Non-Critical} \\ l_2 : \text{request } f[j] \\ l_3 : \text{request } f[j \oplus_n 1] \\ l_4 : \text{Critical} \\ l_5 : \text{release } f[j] \\ l_6 : \text{release } f[j \oplus_n 1] \end{array} \right] \end{array} \right]$				
$\prod_{j=1}^n$	$P[j]$	::		

It is not difficult to verify the following **safety** property

$$\square \neg (at\_l_4[1] \wedge at\_l_4[2]),$$

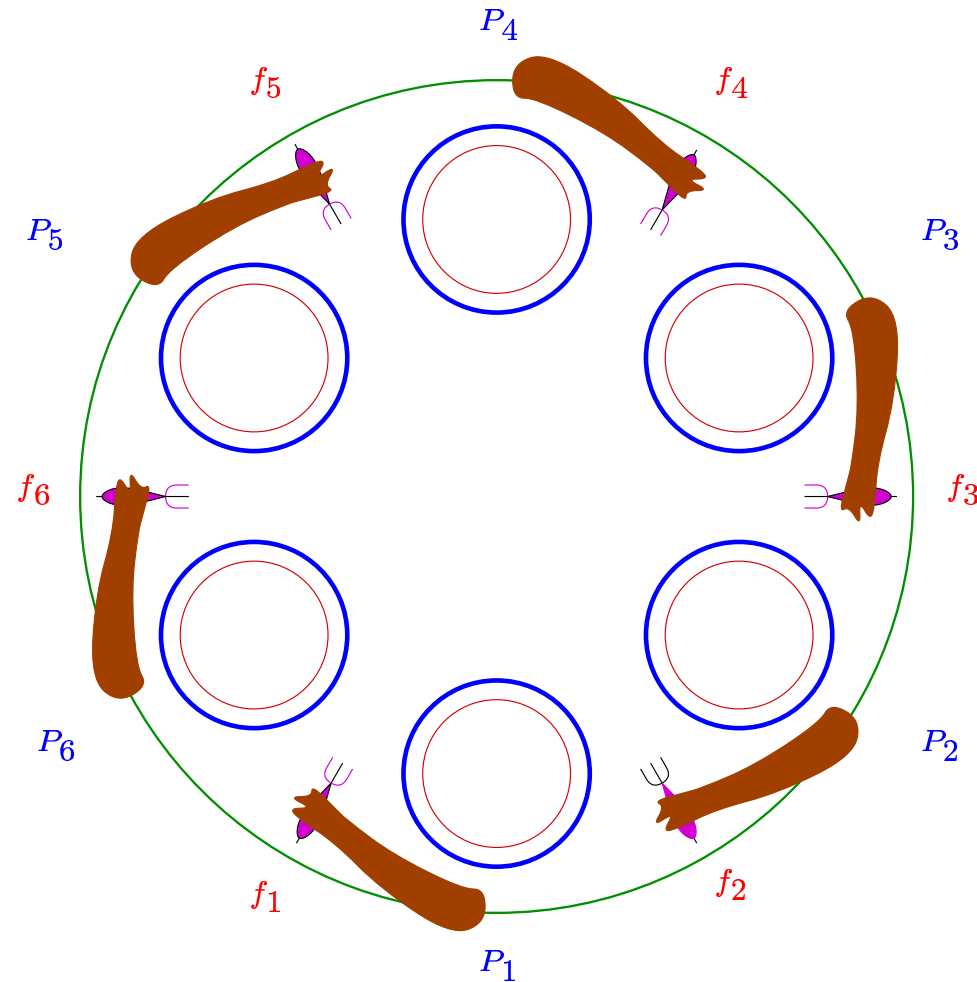
stating that philosophers  $P[1]$  and  $P[2]$  can never eat at the same time.

## Accessibility not Guaranteed

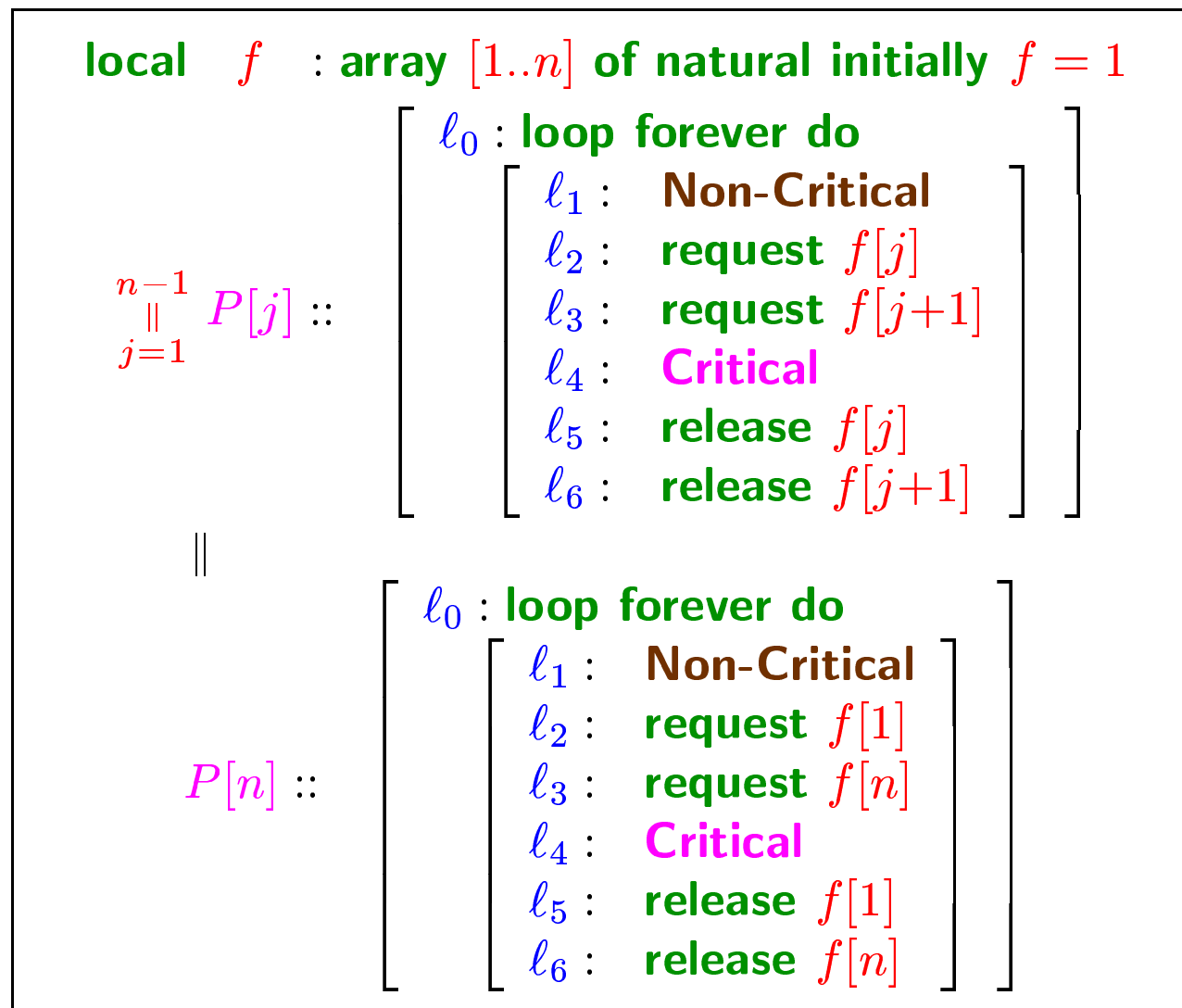
Unfortunately, **Dine** cannot ensure **accessibility** for  $P[1]$ , specifiable by

$$\square (at\_l_2[1] \rightarrow \diamond at\_l_4[1])$$

Because all philosophers may deadlock together.



## Solution: One Contrary Philosopher



Wish to establish **accessibility**, expressible by

$$\psi_{acc}: \quad \square (at\_l_2[j] \rightarrow \diamond (at\_l_4[j]))$$

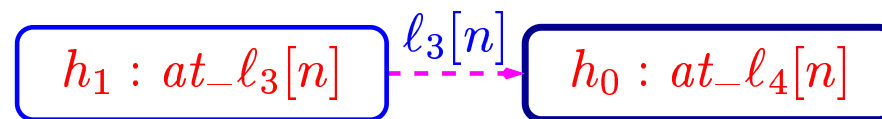
## Prove A Chain of Eventualities

Before proving accessibility for arbitrary  $j$ , we will establish

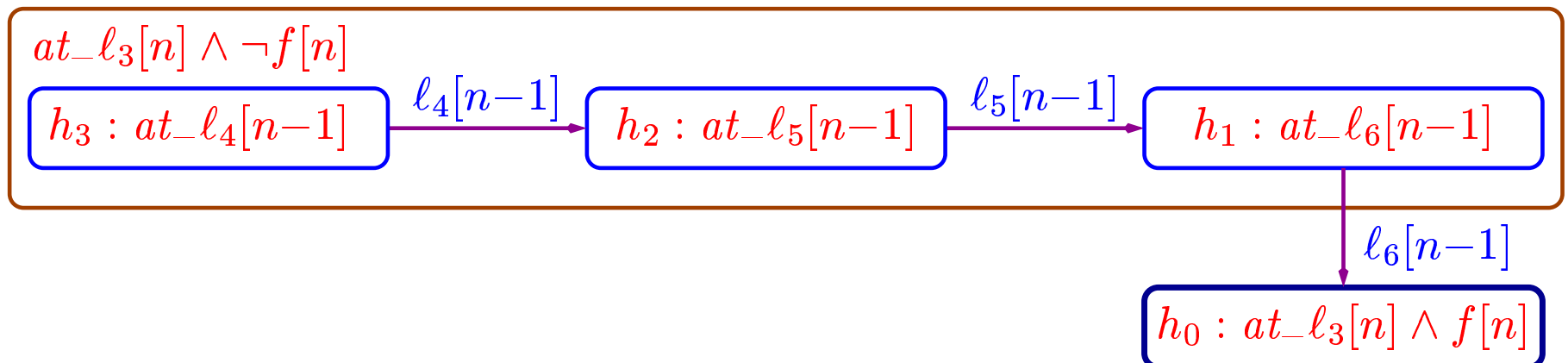
$$A_{3,4}[i] : at\_l_3[i] \Rightarrow \diamond at\_l_4[i]$$

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

**Induction Base:**  $A_{3,4}[n] : at\_l_3[n] \Rightarrow \diamond at\_l_4[n]$

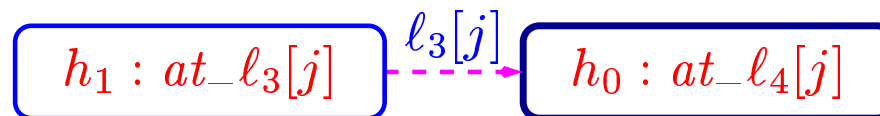


Premise R5 for  $l_3[n]$  requires showing  $at\_l_3[n] \Rightarrow \diamond (at\_l_3[n] \wedge f[n])$ . Using the invariant  $at\_l_{4..6}[n] + at\_l_{4..6}[n-1] + f[n] = 1$ , this can be established by the following verification diagram:



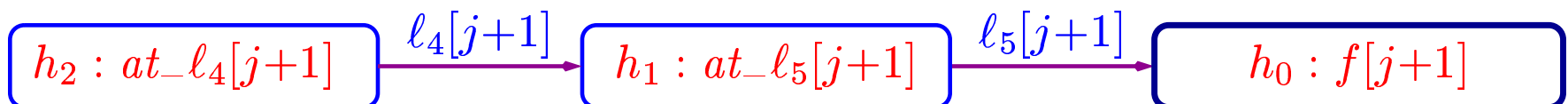
## The Induction Step

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

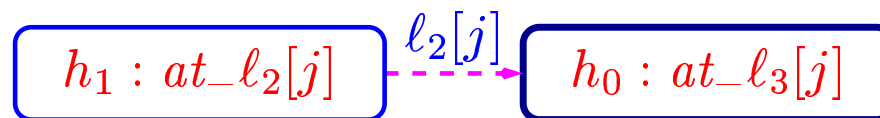


## Verifying Accessibility

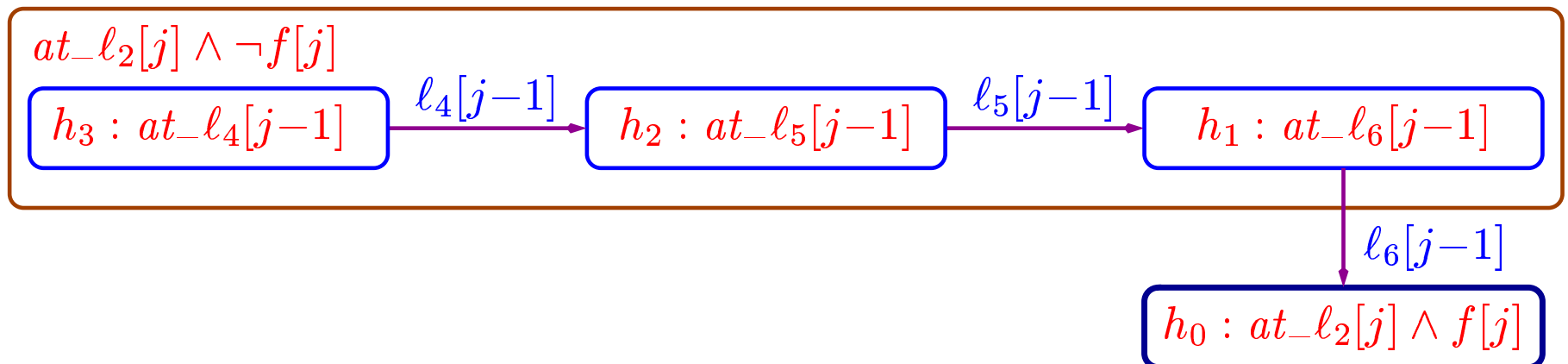
Finally, we verify  $at\_l_2[j] \Rightarrow \diamond at\_l_4[j]$ , for all  $j$ ,  $1 < j < n$ . The proof follows:

1.  $at\_l_2[j] \Rightarrow \diamond at\_l_3[j]$  Verification diagram below
2.  $at\_l_3[j] \Rightarrow \diamond at\_l_4[j]$  Proven by induction
3.  $at\_l_2[j] \Rightarrow \diamond at\_l_4[j]$  Temporal reasoning on 1–2

The verification diagram for  $at\_l_2[j] \Rightarrow \diamond at\_l_3[j]$  is given by:



Premise R5 for  $l_2[j]$  requires showing  $at\_l_2[j] \Rightarrow \diamond (at\_l_2[j] \wedge f[j])$ . Using the invariant  $at\_l_{3..5}[j] + at\_l_{4..6}[j-1] + f[j] = 1$ , 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  $J_1, \dots, J_m$ ,

assertions  $p, q = h_0, h_1, \dots, h_m$ ,

and ranking functions  $\delta_1, \dots, \delta_m : \Sigma \mapsto \mathcal{A}$

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

For  $i = 1, \dots, m$

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

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

$$\text{D4. } h_i \Rightarrow \neg J_i$$

---


$$p \Rightarrow \diamond q$$

## 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:

$$\begin{aligned} V_{\mathcal{J}} &: V \cup \{ \text{nevermore}_i : \text{boolean} \mid (p_i, q_i) \in \mathcal{C} \} \\ \Theta_{\mathcal{J}} &: \Theta \wedge \bigwedge_{(p_i, q_i) \in \mathcal{C}} \neg \text{nevermore}_i \\ \rho_{\mathcal{J}} &: \rho \vee \bigvee_{(p_i, q_i) \in \mathcal{C}} (\text{nevermore}_i := 1) \\ \mathcal{J}_{\mathcal{J}} &: \mathcal{J} \cup \{ \text{nevermore}_i \vee q_i \mid (p_i, q_i) \in \mathcal{C} \} \\ \mathcal{C}_{\mathcal{J}} &: \emptyset \end{aligned}$$

Then, we can use the following reduction:

$$\begin{aligned} \text{In order to prove } \mathcal{D} \models \varphi \Rightarrow \diamond \psi, \text{ it is sufficient to prove} \\ \mathcal{D}_{\mathcal{J}} \models \varphi \Rightarrow \diamond (\psi \vee \bigvee_{(p_i, q_i) \in \mathcal{C}} (p_i \wedge \text{nevermore}_i)). \end{aligned}$$