

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.

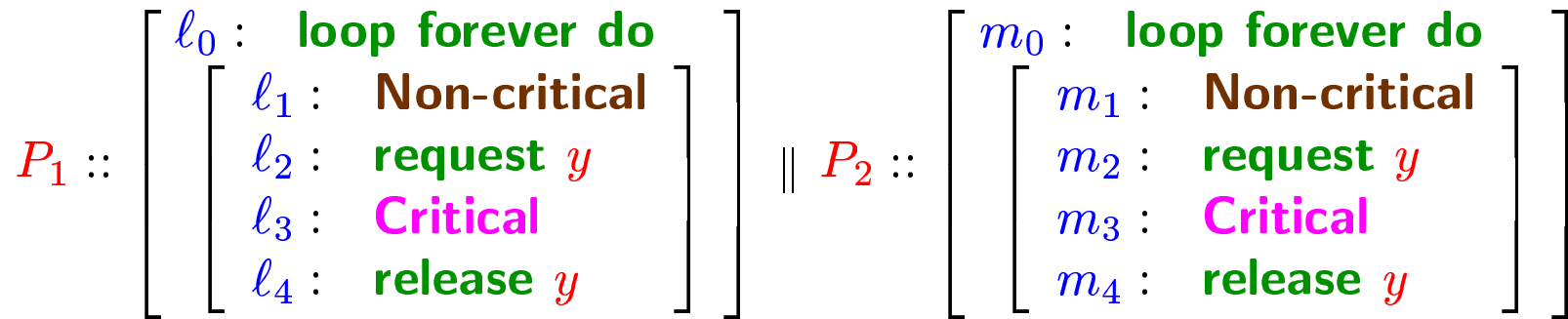
Justification of the Rule

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.

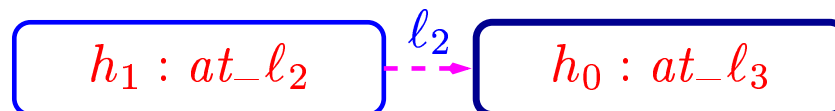
However, there is a certain reduction between the conclusion and the temporal premise. Namely, when establishing the eventual enableness of t_i we only consider computations which never activate t_i itself.

Example: MUX-SEM for 2 Processes

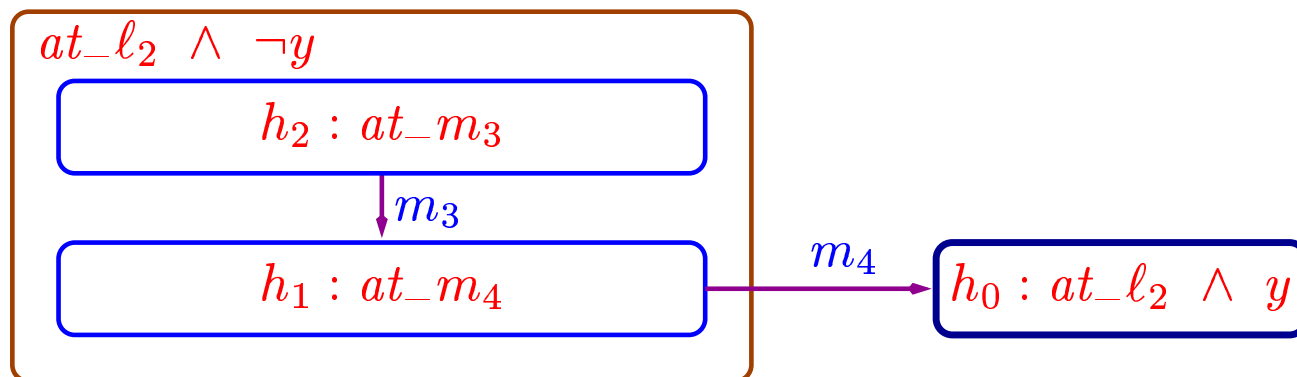
y : natural initially $y = 1$



Following is a verification diagram for the property $at_l_2 \Rightarrow \diamond at_l_3$:

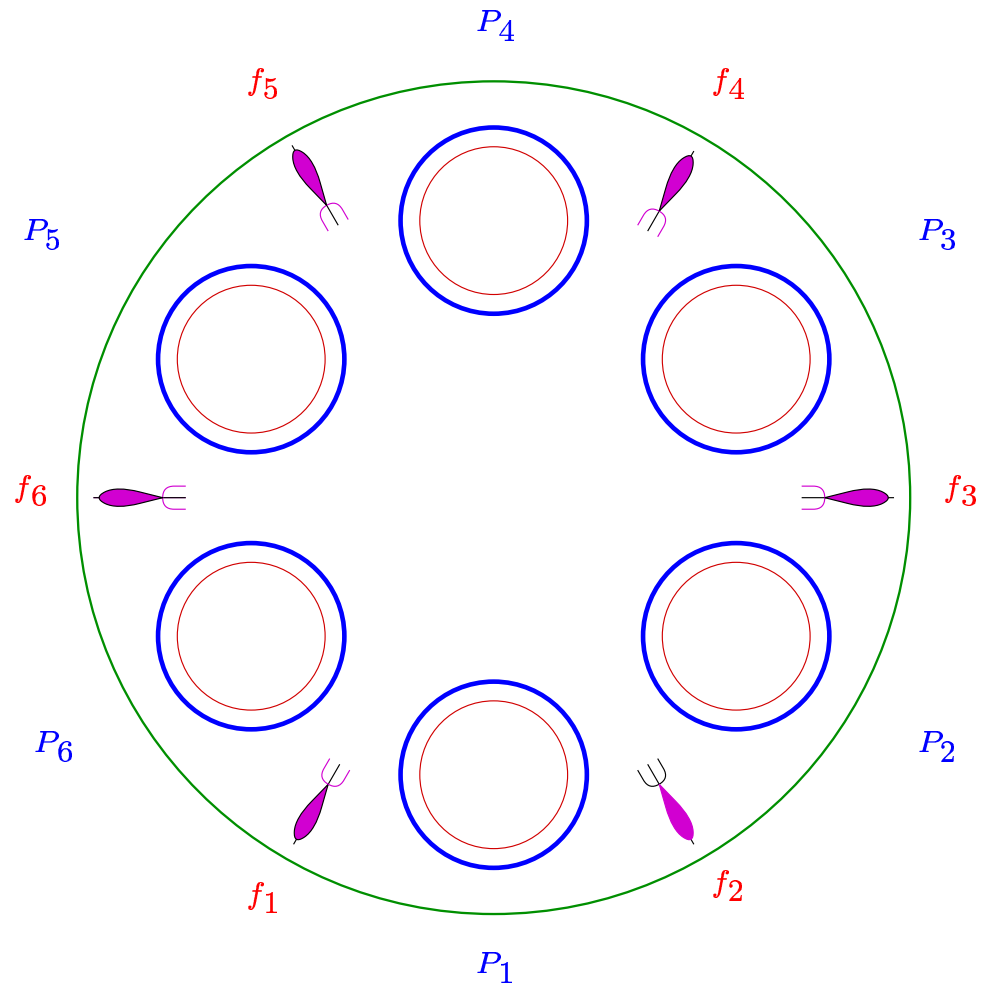


All the verification conditions generated by this verification diagram are non-temporal, except for the instance of premise R5 for transition l_2 which has the form $at_l_2 \Rightarrow \diamond (at_l_2 \wedge y)$. Using the auxiliary invariant $at_l_{3,4} + at_m_{3,4} + y = 1$, the required temporal 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**:

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

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

$$\square \neg (at_l_4[1] \wedge at_l_4[2]),$$

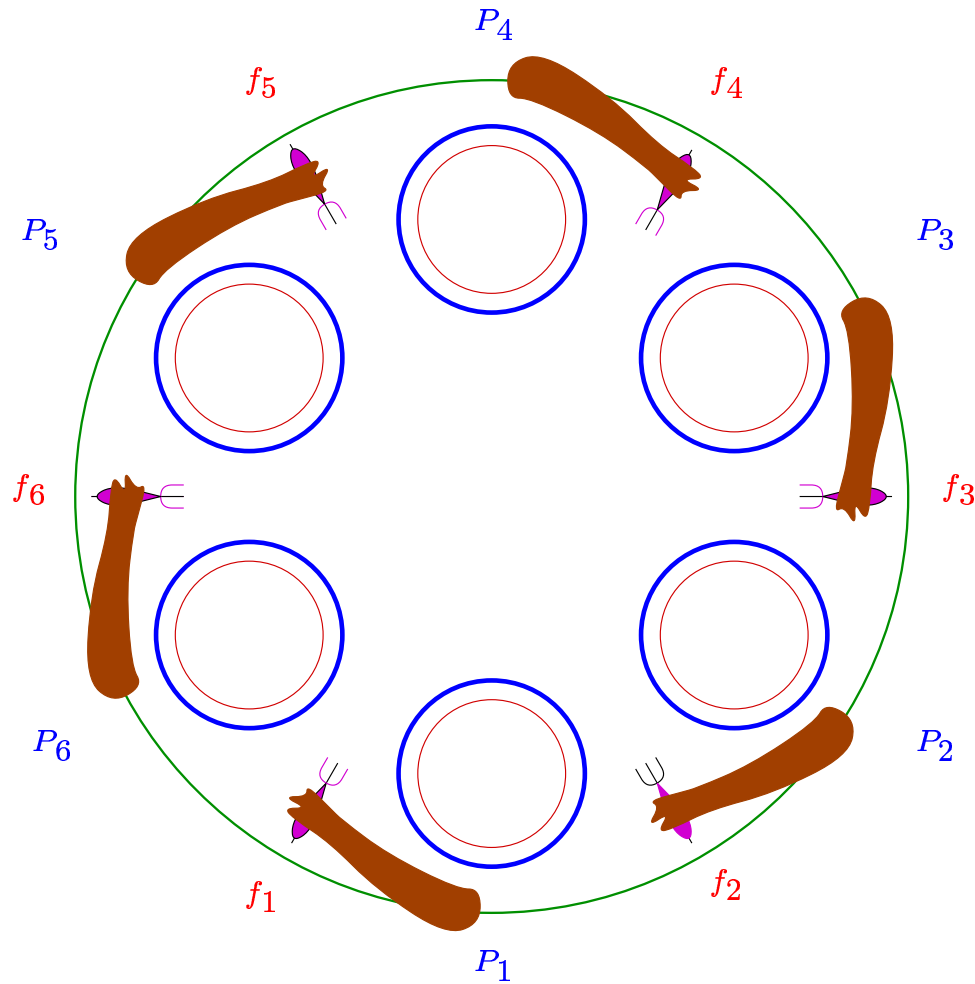
stating that philosophers $P[1]$ and $P[2]$ can never eat at the same time.

Accessibility not Guaranteed

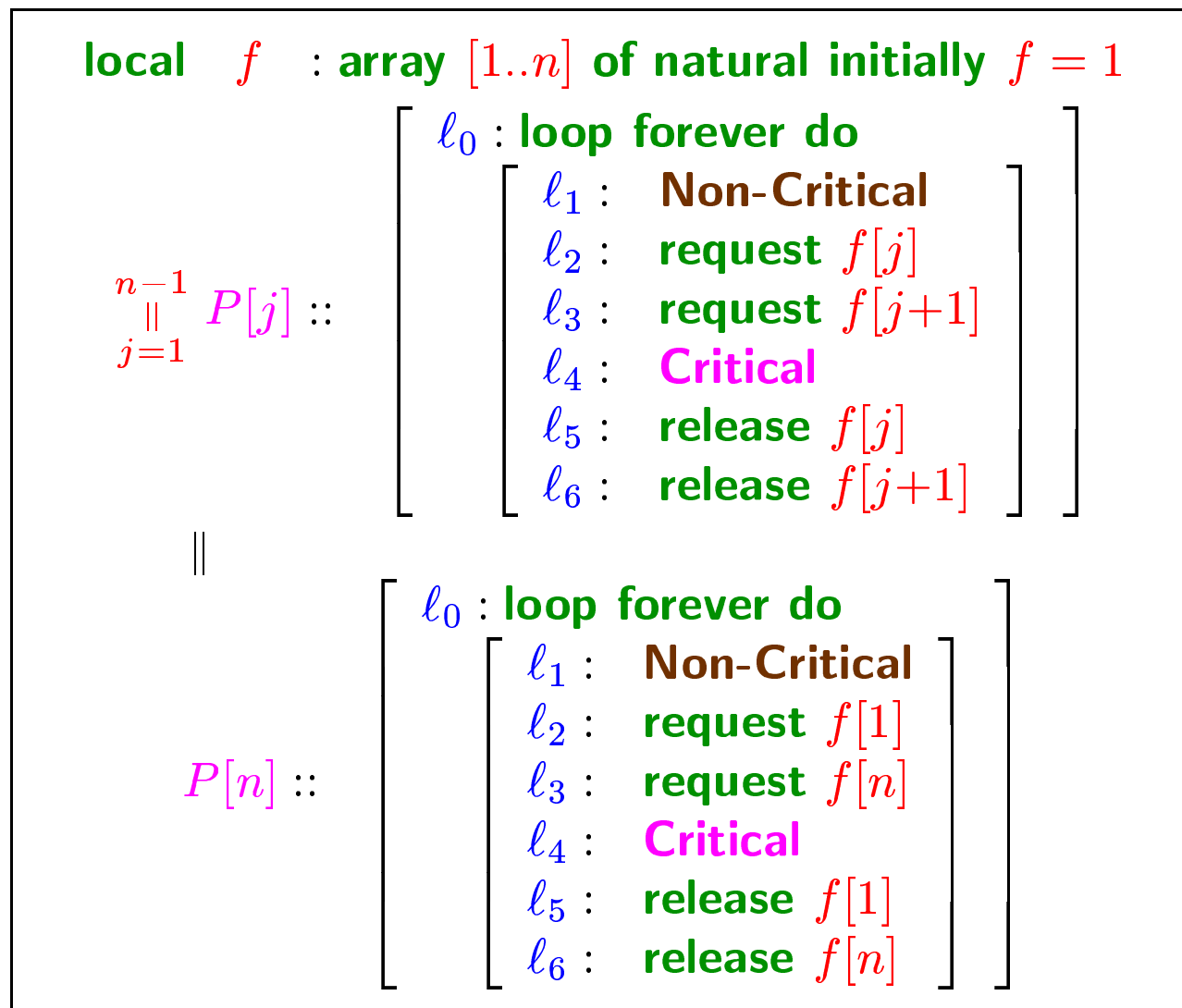
Unfortunately, **Dine** cannot ensure **accessibility** for $P[1]$, specifiable by

$$\square (at_l_2[1] \rightarrow \diamond at_l_4[1])$$

Because all philosophers may deadlock together.



Solution: One Contrary Philosopher



Wish to establish **accessibility**, expressible by

$$\psi_{acc}: \quad \square (at_l_2[j] \rightarrow \diamond (at_l_4[j]))$$

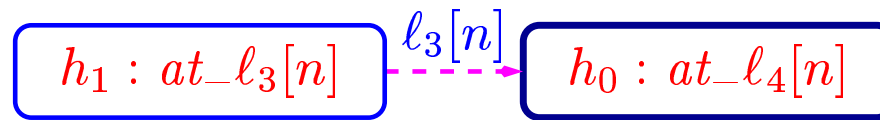
Prove A Chain of Eventualities

Before proving accessibility for arbitrary j , we will establish

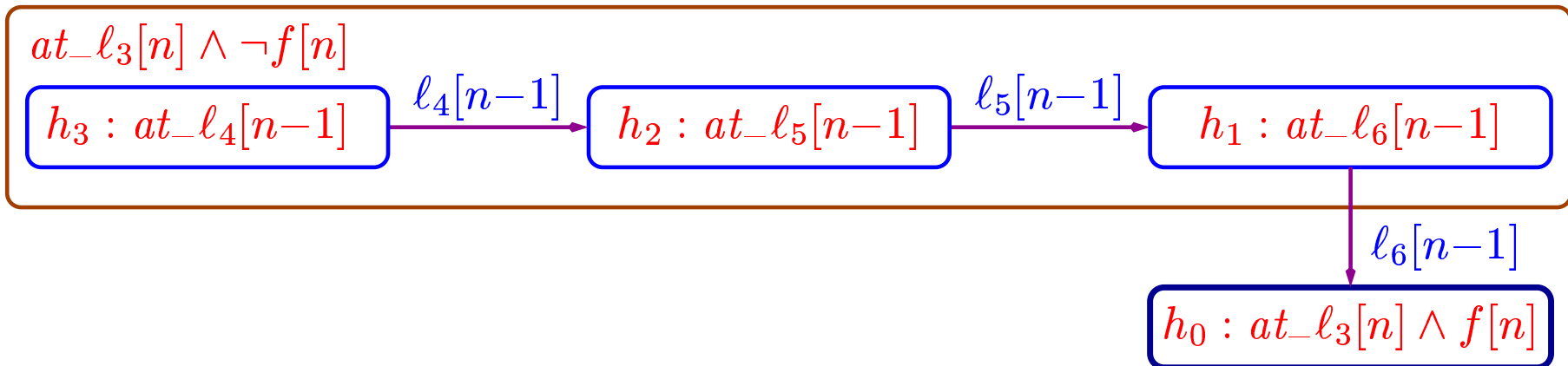
$$A_{3,4}[i] : at_l_3[i] \Rightarrow \diamond at_l_4[i]$$

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

Induction Base: $A_{3,4}[n] : at_l_3[n] \Rightarrow \diamond at_l_4[n]$

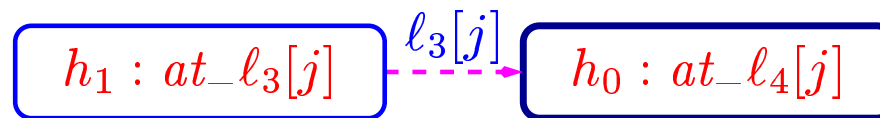


Premise R5 for $l_3[n]$ requires showing $at_l_3[n] \Rightarrow \diamond (at_l_3[n] \wedge f[n])$. Using the invariant $at_l_{4..6}[n] + at_l_{4..6}[n-1] + f[n] = 1$, this can be established by the following verification diagram:



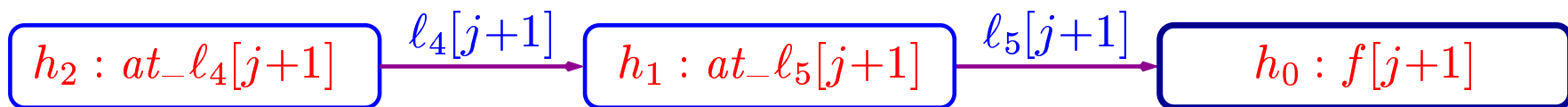
The Induction Step

We will now show that, assuming $A_{3,4}[j+1] : at_{l_3}[j+1] \Rightarrow \diamond at_{l_4}[j+1]$, we can establish $A_{3,4}[j] : at_{l_3}[j] \Rightarrow \diamond at_{l_4}[j]$, for every $j < n$. This is established by the following verification diagram:



Premise R5 for $l_3[j]$ requires showing $at_{l_3}[j] \Rightarrow \diamond (at_{l_3}[j] \wedge f[j+1])$. Using the invariant $at_{l_{4..6}}[j] + at_{l_{3..5}}[j+1] + f[j+1] = 1$, we construct the following proof:

1. $at_{l_3}[j] \Rightarrow at_{l_3}[j+1] \vee at_{l_{4,5}}[j+1] \vee f[j+1]$
According to the invariant
2. $at_{l_3}[j+1] \Rightarrow \diamond at_{l_4}[j+1]$ By induction hypothesis
3. $at_{l_{4,5}}[j+1] \Rightarrow \diamond f[j+1]$ Verification diagram below
4. $at_{l_3}[j] \Rightarrow \diamond f[j+1]$ Temporal reasoning on 1–3

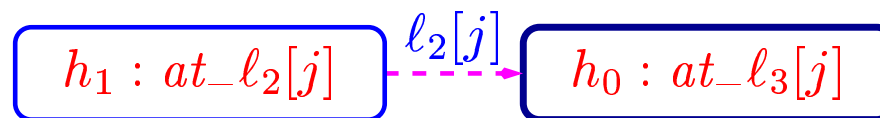


Verifying Accessibility

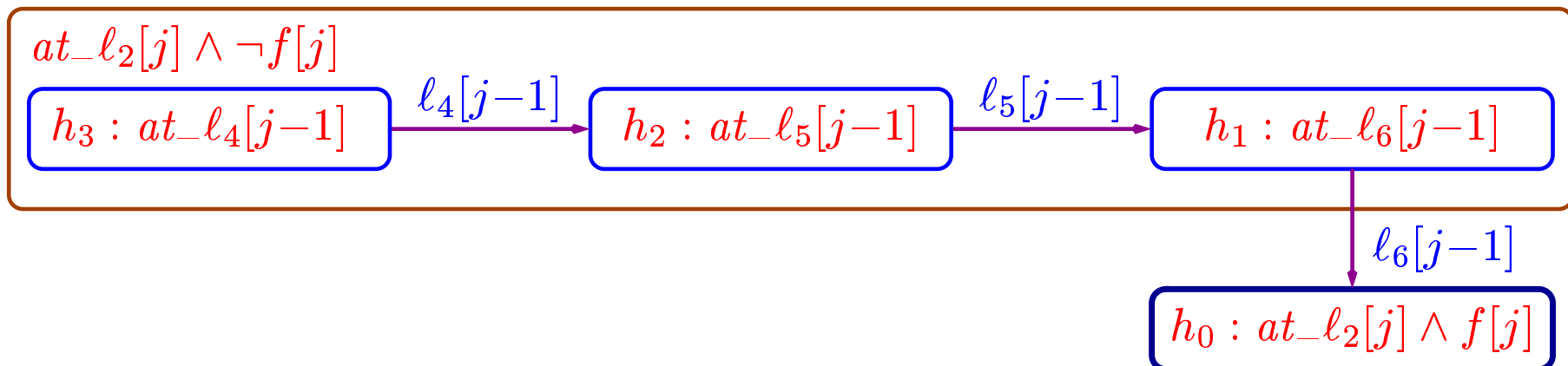
Finally, we verify $at_l_2[j] \Rightarrow \diamond at_l_4[j]$, for all j , $1 < j < n$. The proof follows:

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

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

For $i = 1, \dots, m$

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

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

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

$$p \Rightarrow \diamond q$$

Reducing Compassion to Justice

An alternative approach to the verification of response 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 given by:

$$V_{\mathcal{J}} : V \cup \{ \text{nevermore}_i : \text{boolean} \mid (p_i, q_i) \in \mathcal{C} \}$$

$$\Theta_{\mathcal{J}} : \Theta \wedge \bigwedge_{(p_i, q_i) \in \mathcal{C}} \neg \text{nevermore}_i$$

$$\rho_{\mathcal{J}} : \rho \vee \bigvee_{(p_i, q_i) \in \mathcal{C}} (\text{nevermore}'_i = 1 \wedge \text{pres}(V - \{ \text{nevermore}_i \}))$$

$$\mathcal{J}_{\mathcal{J}} : \mathcal{J} \cup \{ \text{nevermore}_i \vee q_i \mid (p_i, q_i) \in \mathcal{C} \}$$

$$\mathcal{C}_{\mathcal{J}} : \emptyset$$

Then, we can use the following reduction:

In order to prove $\mathcal{D} \models \varphi \Rightarrow \diamond \psi$, it is sufficient to prove

$$\mathcal{D}_{\mathcal{J}} \models \varphi \wedge \neg \text{misprediction} \Rightarrow \diamond (\psi \vee \text{misprediction}),$$

where, $\text{misprediction} = \bigvee_{(p_i, q_i) \in \mathcal{C}} p_i \wedge \text{nevermore}_i$

Justification of the Reduction

The reduction is based on the observation that a state-sequence σ satisfies the compassion requirement (p_i, q_i) if either σ contains only finitely many p_i -states, or it contains infinitely many q_i -states.

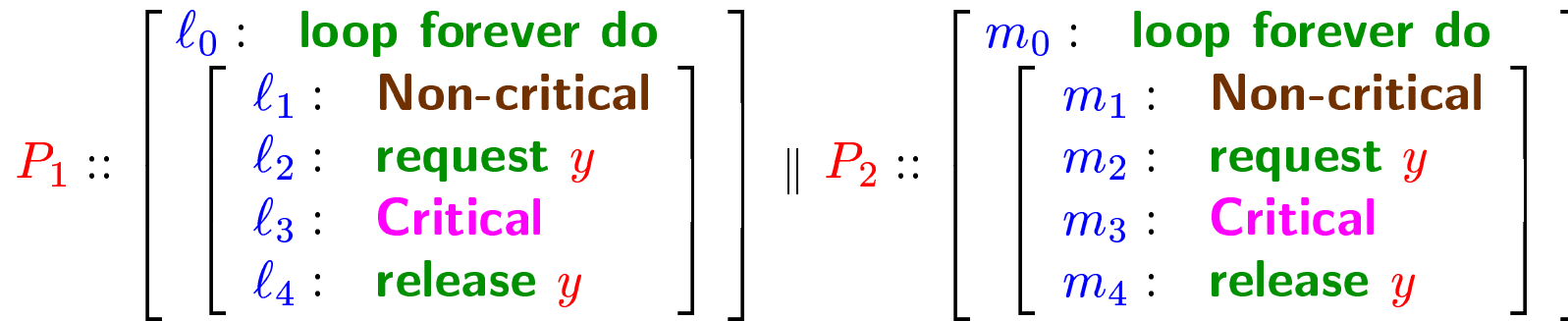
The boolean variable $nevermore_i$ is intended to be set to **1** at a point, beyond which, there will be no further p_i -states. Thus, $nevermore_i$ predicts the absence of p_i -states. If this prediction is correct, then the newly introduced justice requirement $nevermore_i \vee q_i$ is equivalent to the original compassion requirement.

In the revised FDS $\mathcal{D}_{\mathcal{J}}$, the prediction by $nevermore_i$ is implemented as a non-deterministic assignment of **1** to $nevermore_i$. Therefore, the correctness of the prediction cannot be guaranteed.

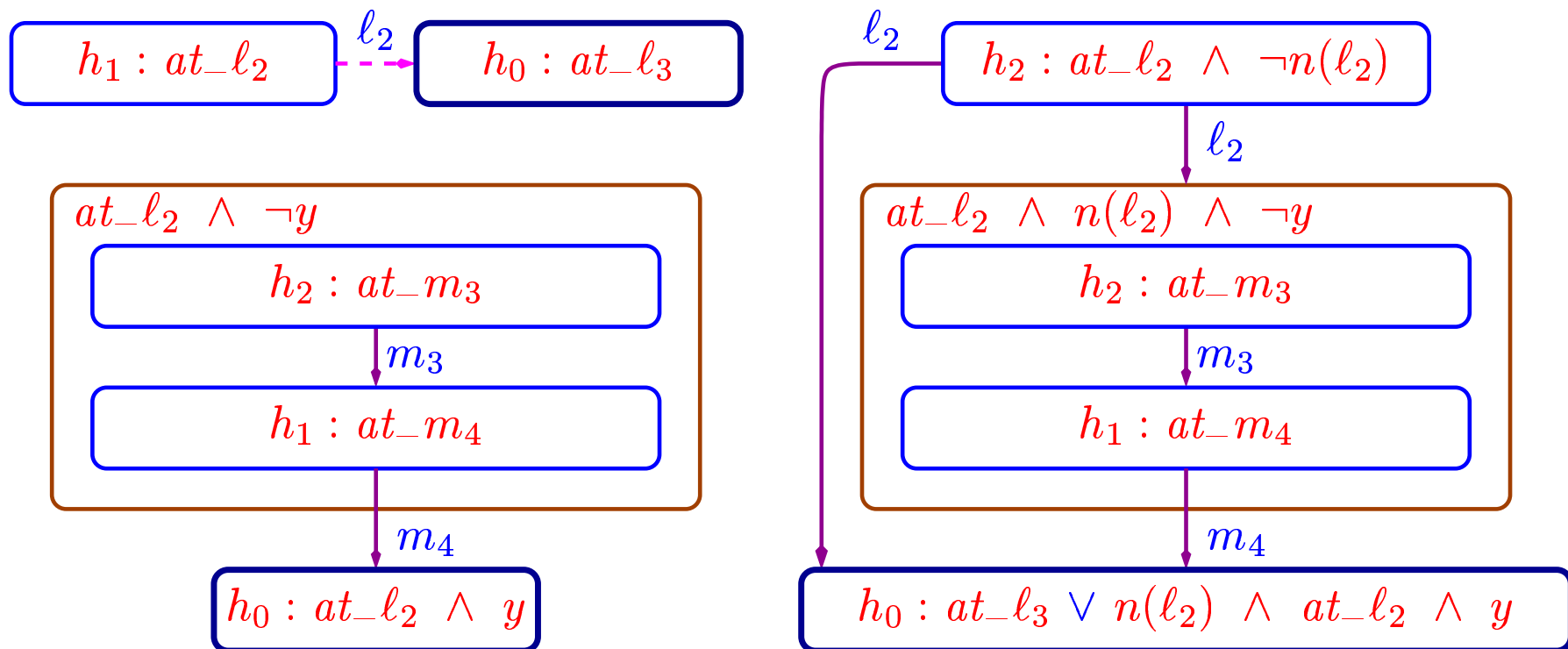
To counter this difficulty, we modify the response property which we aim to prove. The revised property claims that any φ -state in which no mis-prediction has been detected yet, must be followed by a goal state which, either satisfies ψ , or detects a mis-prediction. **Mis-prediction** is identified as a state in which $nevermore_i$ and p_i are both true.

Comparing General Rule RESP to the *nevermore* Reduction

y : natural initially $y = 1$



Following are verification diagrams for the two approaches:



Example: MUX-SEM

Reconsider program MUX-SEM:

<pre> in N : integer where $N > 1$ local y : $\{0, 1\}$ where $y = 1$ $\prod_{p=1}^N P[p] ::$ </pre>	<pre> l_0 : loop forever do l_1 : noncritical l_2 : request y l_3 : critical l_4 : release y </pre>
---	---

For which we wish to prove the response property

$$at_l_2[z] \Rightarrow \diamond at_l_3[z]$$

We start by establishing the following invariants:

$$\begin{aligned}
 \varphi_1 : & \quad \forall i : at_l_{3,4}[i] \rightarrow y = 0 \\
 \varphi_2 : & \quad \forall i \neq j : at_l_{0..2}[i] \vee at_l_{0..2}[j] \quad \text{--- Mutual Exclusion} \\
 \varphi_3 : & \quad y = 0 \rightarrow \exists i : at_l_{3,4}[i]
 \end{aligned}$$

MUX-SEM Continued

Applying the **compassion**→**justice** reduction, we introduce the boolean variables $n[i]$, $i = 1, \dots, N$ (abbreviations for $nevermore[i]$). The added justice requirements are $J_2[i] : n[i] \vee \neg at_l_2[i]$. The **mis-prediction** predicate is given by:

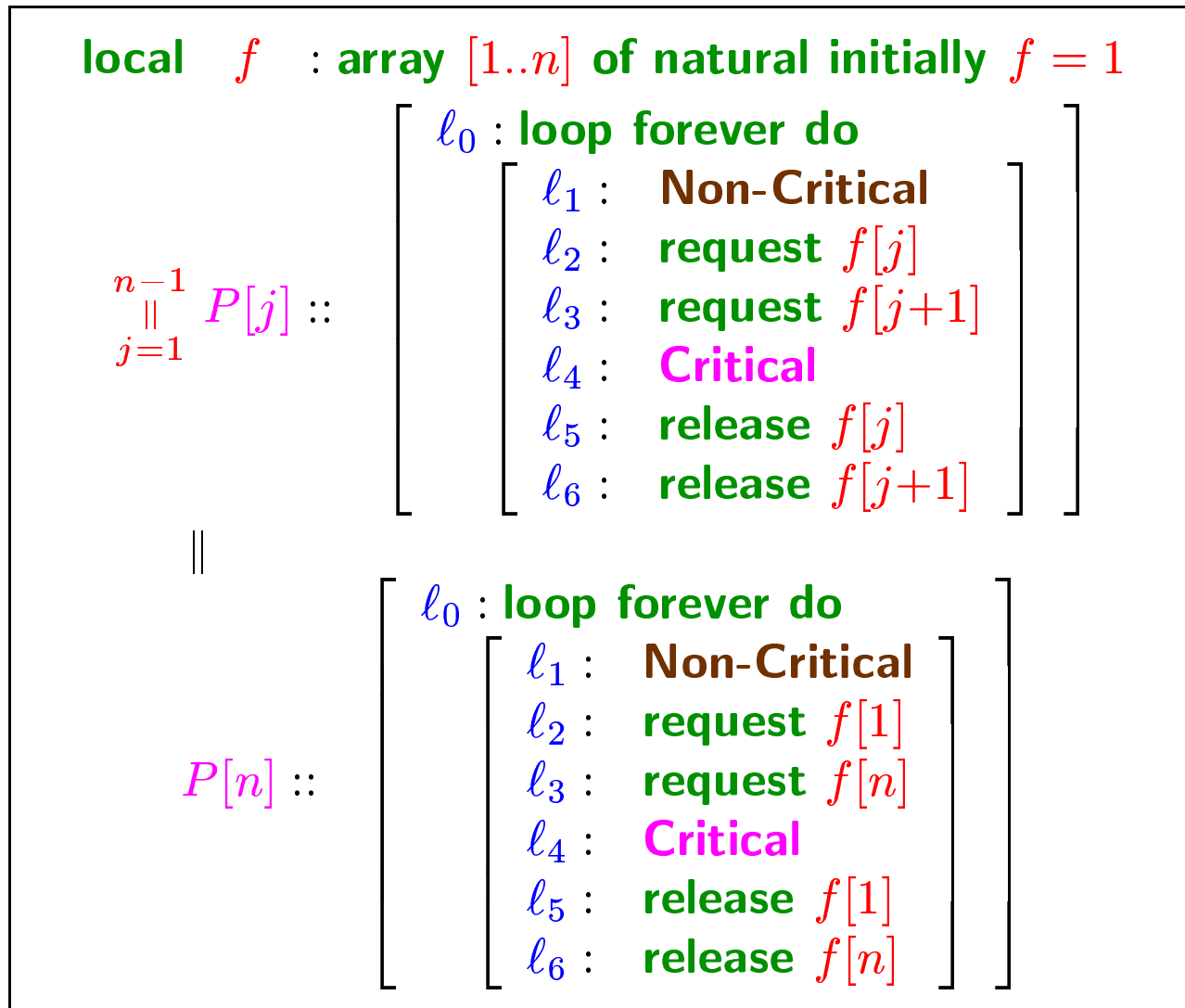
$$misprediction : \bigvee_{i=1}^N at_l_2[i] \wedge y \wedge n[i]$$

The helpful justice requirements for this proof are $J_2[z]$ and $\{J_{3,4}[i] \mid i \in [1..N]\}$. The helpful conditions and ranking functions for these transitions are given in the following table:

Id. p	Requirement	$h(p)$	$\delta(p)$
$J_2[z]$	$n[z] \vee \neg at_l_2[z]$	$at_l_2[z] \wedge \neg n[z]$	$\neg n[z]$
$J_3[i]$	$\neg at_l_3[i]$	$at_l_2[z] \wedge n[z] \wedge at_l_3[i]$	$\neg n[z] \vee at_l_3[i]$
$J_4[i]$	$\neg at_l_4[i]$	$at_l_2[z] \wedge n[z] \wedge at_l_4[i]$	$\neg n[z] \vee at_l_{3,4}[i]$

The ranking functions range over the domain $\{0, 1\}$. The assertion $\delta(p)$ is true at a state if the corresponding ranking of $J(p)$ is 1. Usually, this is the case if requirement p may still become helpful. If $\delta(p)$ is false, then the corresponding ranking is 0.

Example: Dining Philosophers with One Contrary Philosopher



We wish to establish part of **accessibility**, expressible by

$$\psi_{acc}: \quad \square (at_l_3[z] \rightarrow \diamond (at_l_4[z]))$$

for $z \in [2..N - 1]$.

Dining Philosophers Continued

Applying the **compassion**→**justice** reduction, we introduce two arrays of *nevermore* variables, $n_2[i]$ and $n_3[i]$ corresponding to locations $l_2[i]$ and $l_3[i]$.

The helpful justice requirements are $J_{3..6}[z-1]$, $J_{2,3}[z]$, $\{J_{3..5}[i] \mid i \in [z+1..N-1]\}$ and $J_{4..6}[N]$. The helpful conditions for these transitions are given in the following table:

Id. p	$h(p)$
$J_4[z-1]$	$at_l_4[z-1] \wedge at_l_2[z] \wedge n_2[z]$
$J_5[z-1]$	$at_l_5[z-1] \wedge at_l_2[z] \wedge n_2[z]$
$J_6[z-1]$	$at_l_6[z-1] \wedge at_l_2[z] \wedge n_2[z]$
$J_2[z]$	$at_l_2[z] \wedge \neg n_2[z]$
$J_3[z]$	$at_l_3[z] \wedge \neg n_3[z]$
$J_3[i] : i \in [z+1..N-1]$	$at_l_3[z] \wedge at_l_3[i] \wedge \neg n_3[i] \wedge at_l_3[i-1] \wedge n_3[i-1]$
$J_4[i] : i \in [z+1..N-1]$	$at_l_3[z] \wedge at_l_4[i] \wedge \neg n_3[i] \wedge at_l_3[i-1] \wedge n_3[i-1]$
$J_5[i] : i \in [z+1..N-1]$	$at_l_3[z] \wedge at_l_5[i] \wedge \neg n_3[i] \wedge at_l_3[i-1] \wedge n_3[i-1]$
$J_4[N]$	$at_l_3[z] \wedge at_l_4[N] \wedge at_l_3[N-1] \wedge n_3[N-1]$
$J_5[N]$	$at_l_3[z] \wedge at_l_5[N] \wedge at_l_3[N-1] \wedge n_3[N-1]$
$J_6[N]$	$at_l_3[z] \wedge at_l_6[N] \wedge at_l_3[N-1] \wedge n_3[N-1]$

Dining Philosophers: Ranking Functions

The following table presents the distributed ranking functions $\delta(p)$ for each of the helpful requirements $J(p)$. The ranking functions range over $\{0, 1\}$, and the assertion $\delta(p)$ tells us when the ranking of $J(p)$ is 1.

$\delta_4[z-1]$	$n_2[z] \rightarrow at_l_{0..4}[z-1]$
$\delta_5[z-1]$	$n_2[z] \rightarrow at_l_{0..5}[z-1]$
$\delta_6[z-1]$	1
$\delta_2[z]$	$at_l_2[z] \wedge \neg n_2[z]$
$\delta_3[z]$	$\neg n_3[z]$
$\delta_3[i] : i \in [z+1..N-1]$	$\neg n_3[i] \wedge (at_l_3[i-1] \wedge n_3[i-1] \rightarrow at_l_{0..3,6}[i])$
$\delta_4[i] : i \in [z+1..N-1]$	$at_l_3[i-1] \wedge n_3[i-1] \rightarrow at_l_{0..4,6}[i]$
$\delta_5[i] : i \in [z+1..N-1]$	1
$\delta_4[N]$	$at_l_3[N-1] \wedge n_3[N-1] \rightarrow at_l_{0..4}[N]$
$\delta_5[N]$	$at_l_3[N-1] \wedge n_3[N-1] \rightarrow at_l_{0..5}[N]$
$\delta_6[N]$	1

Assignment 1. Draw a verification diagram for the proof of accessibility for the dining-philosophers system.