

EECS3342 Fall 2025
Notes on Discharging POs of Refinement
(New Events: Invariant Preservation & Deadlock Freedom)
Bridge Controller: Initial Model vs. 1st Refinement

CHEN-WEI WANG

Contents

1	Discharging the PO of Invariant Preservation: IL_{in}/inv1.4/INV	2
2	Discharging the PO of Invariant Preservation: IL_{in}/inv1.5/INV	3
3	Discharging the PO of Relative Deadlock Freedom	4

1 Discharging the PO of Invariant Preservation: IL.in/inv1_4/INV

$$\begin{array}{l}
 d \in \mathbb{N} \\
 d > 0 \\
 n \in \mathbb{N} \\
 n \leq d \\
 a \in \mathbb{N} \\
 b \in \mathbb{N} \\
 c \in \mathbb{N} \\
 a + b + c = n \\
 a = 0 \vee c = 0 \\
 a > 0 \\
 \perp \\
 (a - 1) + (b + 1) + c = n
 \end{array}$$

MON

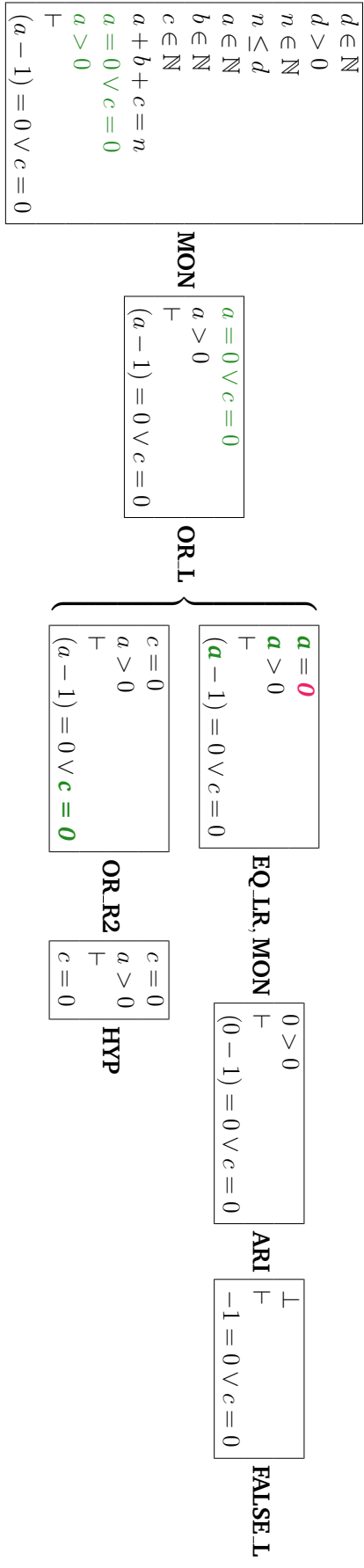
$$\begin{array}{l}
 a + b + c = n \\
 \perp \\
 (a - 1) + (b + 1) + c = n
 \end{array}$$

ARI

$$\begin{array}{l}
 a + b + c = n \\
 \perp \\
 a + b + c = n
 \end{array}$$

HYP

2 Discharging the PO of Invariant Preservation: IL.in/inv1_5/INV



3 Discharging the PO of Relative Deadlock Freedom

$$\begin{array}{l}
 d \in \mathbb{N} \\
 d > 0 \\
 n \in \mathbb{N} \\
 n \leq d \\
 a \in \mathbb{N} \\
 b \in \mathbb{N} \\
 c \in \mathbb{N} \\
 a + b + c = n \\
 a = 0 \vee c = 0 \\
 n < d \vee n > 0 \\
 \vdash \\
 a + b < d \wedge c = 0 \\
 \vee c > 0 \\
 \vee a > 0 \\
 \vee b > 0 \wedge a = 0
 \end{array}$$

MON

$$\begin{array}{l}
 d > 0 \\
 a \in \mathbb{N} \\
 b \in \mathbb{N} \\
 c \in \mathbb{N} \\
 \vdash \\
 a + b < d \wedge c = 0 \\
 \vee c > 0 \\
 \vee a > 0 \\
 \vee b > 0 \wedge a = 0
 \end{array}$$

OR.R,ARI

$$\begin{array}{l}
 d > 0 \\
 a \in \mathbb{N} \\
 b \in \mathbb{N} \\
 c = 0 \\
 \vdash \\
 a + b < d \wedge c = 0 \\
 \vee c > 0 \\
 \vee a > 0 \\
 \vee b > 0 \wedge a = 0
 \end{array}$$

EQ.LR,MON

$$\begin{array}{l}
 d > 0 \\
 a \in \mathbb{N} \\
 b \in \mathbb{N} \\
 \vdash \\
 a + b < d \wedge 0 = 0 \\
 \vee 0 > 0 \\
 \vee a > 0 \\
 \vee b > 0 \wedge a = 0
 \end{array}$$

OR.R,
ARI

$$\begin{array}{l}
 d > 0 \\
 a = 0 \\
 b \in \mathbb{N} \\
 \vdash \\
 a + b < d \wedge 0 = 0 \\
 \vee b > 0 \wedge a = 0
 \end{array}$$

EQ.LR,
MON

$$\begin{array}{l}
 d > 0 \\
 b \in \mathbb{N} \\
 \vdash \\
 0 + b < d \wedge 0 = 0 \\
 \vee b > 0 \wedge 0 = 0
 \end{array}$$

ARI

$$\begin{array}{l}
 d > 0 \\
 \vdash \\
 b = 0 \vee b > 0 \\
 b < d \wedge 0 = 0 \\
 \vee b > 0 \wedge 0 = 0
 \end{array}$$

OR.L

$$\left\{ \begin{array}{l}
 \begin{array}{l}
 d > 0 \\
 b = 0 \\
 \vdash \\
 b < d \wedge 0 = 0 \\
 \vee b > 0 \wedge 0 = 0
 \end{array} \\
 \text{OR.R1} \\
 \begin{array}{l}
 d > 0 \\
 b = 0 \\
 \vdash \\
 b < d \wedge 0 = 0
 \end{array} \\
 \text{OR.R1, MON} \\
 \begin{array}{l}
 d > 0 \\
 \vdash \\
 0 < d \wedge 0 = 0
 \end{array} \\
 \text{AND.R} \\
 \left\{ \begin{array}{l}
 \begin{array}{l}
 d > 0 \\
 0 < d
 \end{array} \\
 \begin{array}{l}
 d > 0 \\
 0 = 0
 \end{array} \\
 \text{ARI, HYP} \\
 \text{EQ}
 \end{array} \right. \\
 \end{array} \right\}$$

$$\left\{ \begin{array}{l}
 \begin{array}{l}
 d > 0 \\
 b > 0 \\
 \vdash \\
 b < d \wedge 0 = 0 \\
 \vee b > 0 \wedge 0 = 0
 \end{array} \\
 \text{OR.R2} \\
 \begin{array}{l}
 d > 0 \\
 b > 0 \\
 \vdash \\
 b > 0 \wedge 0 = 0
 \end{array} \\
 \text{AND.R} \\
 \left\{ \begin{array}{l}
 \begin{array}{l}
 d > 0 \\
 b > 0 \\
 \vdash \\
 b > 0 \\
 0 = 0
 \end{array} \\
 \begin{array}{l}
 d > 0 \\
 b > 0 \\
 \vdash \\
 0 = 0
 \end{array} \\
 \text{HYP} \\
 \text{EQ}
 \end{array} \right.
 \end{array} \right\}$$