

EECS3342 Fall 2025
Notes on Discharging POs of Refinement
(Guard Strengthening & Invariant Preservation)
Bridge Controller: Initial Model vs. 1st Refinement

CHEN-WEI WANG

Contents

1	Discharging the PO of Guard Strengthening: ML_out/GRD	2
2	Discharging the PO of Guard Strengthening: ML_in/GRD	3
3	Discharging the PO of Invariant Preservation: ML_out/inv1_4/INV	4
4	Discharging the PO of Invariant Preservation: ML_in/inv1_5/INV	5

1 Discharging the PO of Guard Strengthening: ML.out/GRD

$d \in \mathbb{N}$
 $d > 0$
 $n \in \mathbb{N}$
 $n \leq d$
 $a \in \mathbb{N}$
 $b \in \mathbb{N}$
 $c \in \mathbb{N}$
 $a + b + c = n$
 $a = 0 \vee c = 0$
 $a + b < d$
 $c = 0$
 $\perp$
 $n < d$

MON

$a + b + c = n$
 $a + b < d$
 $c = 0$
 $\perp$
 $n < d$

EQ_LR, MON

$a + b + c = n$
 $a + b < d$
 $\perp$
 $n < d$

ARI

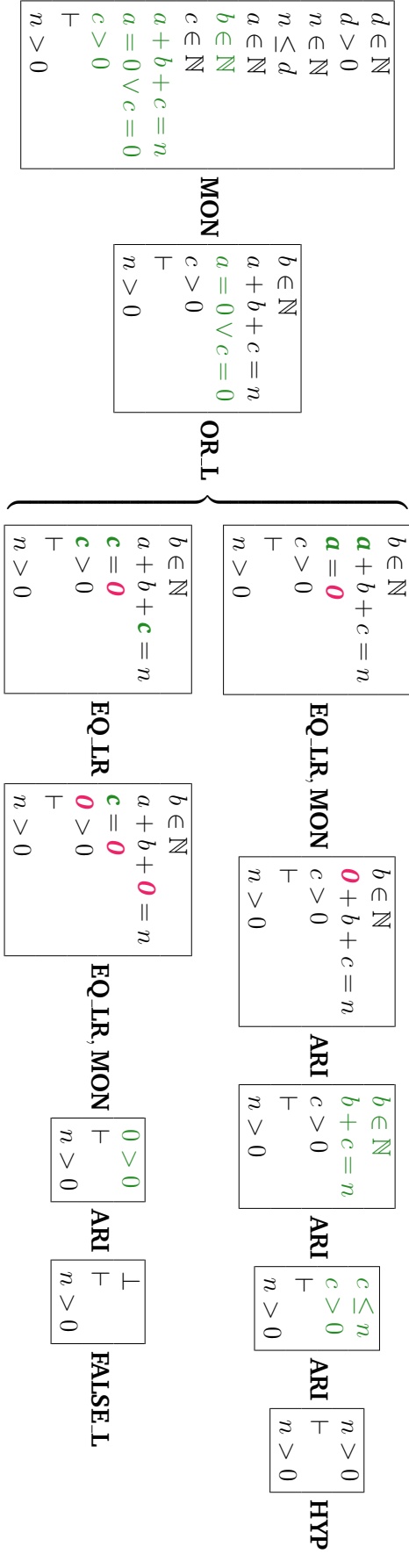
$a + b = n$
 $a + b < d$
 $\perp$
 $n < d$

EQ_LR, MON

$n < d$
 $\perp$
 $n < d$

HYP

2 Discharging the PO of Guard Strengthening: ML in/GRD



3 Discharging the PO of Invariant Preservation: ML.out/inv1_4/INV

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

MON

$$\begin{array}{l} a + b + c = n \\ \vdash \\ \textcolor{teal}{(a + 1) + b + c = (n + 1)} \end{array}$$

ARI

$$\begin{array}{l} \textcolor{teal}{a + b + c} = \textcolor{violet}{n} \\ \vdash \\ \textcolor{teal}{a + b + c} + 1 = n + 1 \end{array}$$

EQ_LR, MON

$$\begin{array}{l} \vdash \\ n + 1 = n + 1 \end{array}$$

EQ

4 Discharging the PO of Invariant Preservation: ML.in/inv1_5/INV

