

EECS3342 Winter 2023
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

$d \in \mathbb{N}$
 $d > 0$
 $n \in \mathbb{N}$
 $n \leq d$
 $a \in \mathbb{N}$
 $b \in \mathbb{N}$
 $c \in \mathbb{N}$
 $a + b + c = n$
 $a = 0 \vee c = 0$
 $a > 0$
 \vdash
 $(a - 1) + (b + 1) + c = n$

MON

$a + b + c = n$
 \vdash
 $(a - 1) + (b + 1) + c = n$

ARI

$a + b + c = n$
 \vdash
 $a + b + c = n$

HYP

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

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$
$n < d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \vee c = 0$
$a > 0$
\vdash
$(a-1) = 0 \vee c = 0$

MON

$a = 0 \vee c = 0$
$a > 0$
\vdash
$(a-1) = 0 \vee c = 0$

OR L

$a = 0$
$a > 0$
\vdash
$(a-1) = 0 \vee c = 0$

$c = 0$
$a > 0$
\vdash
$(a-1) = 0 \vee c = 0$

EQ LR, MON

$0 > 0$
\vdash
$(0-1) = 0 \vee c = 0$

ARI

\vdash
\vdash
$-1 = 0 \vee c = 0$

FALSE L

OR R2

$c = 0$
$a > 0$
\vdash
$c = 0$

HYP

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

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

OR.L

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

OR.R1

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

OR.R1, MON

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

AND.R

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

ARI, HYP

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

OR.R2

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

AND.R

$$\begin{array}{l}
 d > 0 \\
 b > 0 \\
 \vdash \\
 b > 0
 \end{array}$$

HYP

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

EQ