

EECS3342 Winter 2022  
Notes on Discharging POs of Refinement  
(New Events: Invariant Preservation & Deadlock Freedom)  
Bridge Controller: Initial Model vs. 1st Refinement

CHEN-WEI WANG

## Contents

1 Discharing the PO of Invariant Preservation: IL_in/inv1_4/INV	2
2 Discharing the PO of Invariant Preservation: IL_in/inv1_5/INV	3
3 Discharing the PO of Relative Deadlock Freedom	5

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

**MON**

$a + b + c = n$
$\top$
$\textcolor{green}{(a - 1) + (b + 1) + c = n}$

**ARI**

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

**HYP**

## 2 Discharging the PO of Invariant Preservation: II\_im/inv1\_5/INV

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

MON

$\textcolor{green}{a = 0 \vee c = 0}$   
 $a > 0$   
 $\top$   
 $(a - 1) = 0 \vee c = 0$

OR\_L

$\textcolor{red}{a = 0}$   
 $\textcolor{green}{a > 0}$   
 $\top$   
 $(\textcolor{red}{a} - 1) = 0 \vee c = 0$

EQ\_LR, MON

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

ARI

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

FALSE\_L

$c = 0$   
 $a > 0$   
 $\top$   
 $(a - 1) = 0 \vee \textcolor{green}{c = 0}$

OR\_R2

$c = 0$   
 $a > 0$   
 $\top$   
 $c = 0$

HYP

### 3 Discharging the PO of Relative Deadlock Freedom

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

MON

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

OR.R, ARI

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

EQ.LR, MON

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

OR.R,  
ARI

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

EQ.LR,  
MON

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

$d > 0$   
 $b = 0 \vee b > 0$   
 $\vdash$   
 $b < d \wedge 0 = 0$   
 $\vee b > 0 \wedge 0 = 0$

OR.L

$d > 0$   
 $b = 0$   
 $\vdash$   
 $b < d \wedge 0 = 0$   
 $\vee b > 0 \wedge 0 = 0$

OR.R1

$d > 0$   
 $b = 0$   
 $\vdash$   
 $b < d \wedge 0 = 0$

OR.R1,  
MON

$d > 0$   
 $\vdash$   
 $0 < d \wedge 0 = 0$

$d > 0$   
 $\vdash$   
 $0 < d$   
 $d > 0$   
 $\vdash$   
 $0 = 0$

ARI,  
HYP

EQ

$d > 0$   
 $b > 0$   
 $\vdash$   
 $b < d \wedge 0 = 0$   
 $\vee b > 0 \wedge 0 = 0$

OR.R2

$d > 0$   
 $b > 0$   
 $\vdash$   
 $b > 0 \wedge 0 = 0$

AND.R

$d > 0$   
 $b > 0$   
 $\vdash$   
 $b > 0$   
 $d > 0$   
 $b > 0$   
 $\vdash$   
 $0 = 0$

HYP

EQ