

EECS3342 Fall 2025
Notes on Discharging POs of Refinement
Invariant Preservation, Convergence, Deadlock Freedom
Bridge Controller: 2nd Refinement

CHEN-WEI WANG

Contents

1	Discharging the PO of Invariant Preservation: ML_out/inv2_4/INV (1st Attempt)	2
2	Discharging the PO of Invariant Preservation: IL_out/inv2_3/INV (1st Attempt)	3
3	Discharging the PO of Invariant Preservation: ML_out/inv2_4/INV (2nd Attempt)	4
4	Discharging the PO of Invariant Preservation: IL_out/inv2_3/INV (2nd Attempt)	5

1 Discharging the PO of Invariant Preservation: ML.out/inv2.4/INV (1st Attempt)

$d \in \mathbb{N}$
 $d > 0$
 $COLOUR = \{green, red\}$
 $green \neq red$
 $n \in \mathbb{N}$
 $n \leq d$
 $a \in \mathbb{N}$
 $b \in \mathbb{N}$
 $c \in \mathbb{N}$
 $a + b + c = n$
 $a = 0 \vee c = 0$
 $ml_hl \in COLOUR$
 $il_hl \in COLOUR$
 $ml_hl = green \Rightarrow a + b < d \wedge c = 0$
 $il_hl = green \Rightarrow b > 0 \wedge a = 0$
 $ml_hl = green$
 $\vdash$
 $il_hl = green \Rightarrow b > 0 \wedge (a + 1) = 0$

MON

$green \neq red$
 $il_hl = green \Rightarrow b > 0 \wedge a = 0$
 $ml_hl = green$
 $\vdash$
 $il_hl = green \Rightarrow b > 0 \wedge (a + 1) = 0$

IMP_R

$green \neq red$
 $il_hl = green \Rightarrow b > 0 \wedge a = 0$
 $ml_hl = green$
 $il_hl = green$
 $\vdash$
 $b > 0 \wedge (a + 1) = 0$

IMP_L

$green \neq red$
 $b > 0 \wedge a = 0$
 $ml_hl = green$
 $il_hl = green$
 $\vdash$
 $b > 0 \wedge (a + 1) = 0$

AND_L

$green \neq red$
 $b > 0$
 $a = 0$
 $ml_hl = green$
 $il_hl = green$
 $\vdash$
 $b > 0 \wedge (a + 1) = 0$

AND_R

$green \neq red$
 $b > 0$
 $a = 0$
 $ml_hl = green$
 $il_hl = green$
 $\vdash$
 $b > 0$

HYP

$green \neq red$
 $b > 0$
 $a = 0$
 $ml_hl = green$
 $il_hl = green$
 $\vdash$
 $green \neq red$
 $b > 0$
 $a = 0$
 $ml_hl = green$
 $il_hl = green$
 $(a + 1) = 0$

EQ_LR,
MON

$green \neq red$
 $ml_hl = green$
 $il_hl = green$
 $\vdash$
 $(0 + 1) = 0$

ARI

$green \neq red$
 $ml_hl = green$
 $il_hl = green$
 $\vdash$
 $1 = 0$

??

2 Discharging the PO of Invariant Preservation: IL.out/inv2.3/INV (1st Attempt)

$d \in \mathbb{N}$
 $d > 0$
 $COLOUR = \{green, red\}$
 $green \neq red$
 $n \in \mathbb{N}$
 $n \leq d$
 $a \in \mathbb{N}$
 $b \in \mathbb{N}$
 $c \in \mathbb{N}$
 $a + b + c = n$
 $a = 0 \vee c = 0$
 $ml_tl \in COLOUR$
 $il_tl \in COLOUR$
 $ml_tl = green \Rightarrow a + b < d \wedge c = 0$
 $il_tl = green \Rightarrow b > 0 \wedge a = 0$
 $il_tl = green$
 $\vdash$
 $ml_tl = green \Rightarrow a + (b - 1) < d \wedge (c + 1) = 0$

MON

$green \neq red$
 $ml_tl = green \Rightarrow a + b < d \wedge c = 0$
 $il_tl = green$
 $\vdash$
 $ml_tl = green \Rightarrow a + (b - 1) < d \wedge (c + 1) = 0$

IMP_R

$green \neq red$
 $ml_tl = green \Rightarrow a + b < d \wedge c = 0$
 $il_tl = green$
 $ml_tl = green$
 $\vdash$
 $a + (b - 1) < d \wedge (c + 1) = 0$

IMP_L

$green \neq red$
 $a + b < d \wedge c = 0$
 $il_tl = green$
 $ml_tl = green$
 $\vdash$
 $a + (b - 1) < d \wedge (c + 1) = 0$

AND_L

$green \neq red$
 $a + b < d$
 $c = 0$
 $il_tl = green$
 $ml_tl = green$
 $\vdash$
 $a + (b - 1) < d \wedge (c + 1) = 0$

AND_R

$green \neq red$
 $a + b < d$
 $c = 0$
 $il_tl = green$
 $ml_tl = green$
 $\vdash$
 $a + (b - 1) < d$
 $green \neq red$
 $a + b < d$
 $c = 0$
 $il_tl = green$
 $ml_tl = green$
 $\vdash$
 $(c + 1) = 0$

MON

$a + b < d$
 $\vdash$
 $a + (b - 1) < d$

ARI

EQ_LR, MON

$green \neq red$
 $il_tl = green$
 $ml_tl = green$
 $\vdash$
 $(0 + 1) = 0$

ARI

$green \neq red$
 $il_tl = green$
 $ml_tl = green$
 $\vdash$
 $1 = 0$

??

3 Discharging the PO of Invariant Preservation: ML.out/inv2.4/INV (2nd Attempt)

$d \in \mathbb{N}$
 $d > 0$
 $COLOUR = \{green, red\}$
 $green \neq red$
 $n \in \mathbb{N}$
 $n \leq d$
 $a \in \mathbb{N}$
 $b \in \mathbb{N}$
 $c \in \mathbb{N}$
 $a + b + c = n$
 $a = 0 \vee c = 0$
 $ml_lI \in COLOUR$
 $il_lI \in COLOUR$
 $ml_lI = green \Rightarrow a + b < d \wedge c = 0$
 $il_lI = green \Rightarrow b > 0 \wedge a = 0$
 $ml_lI = red \vee il_lI = red$
 $ml_lI = green$
 $\vdash$
 $il_lI = green \Rightarrow b > 0 \wedge (a + 1) = 0$

MON

$green \neq red$
 $il_lI = green \Rightarrow b > 0 \wedge a = 0$
 $ml_lI = red \vee il_lI = red$
 $ml_lI = green$
 $\vdash$
 $il_lI = green \Rightarrow b > 0 \wedge (a + 1) = 0$

IMP R

$green \neq red$
 $il_lI = green \Rightarrow b > 0 \wedge a = 0$
 $ml_lI = green$
 $ml_lI = red \vee il_lI = red$
 $il_lI = green$
 $\vdash$
 $b > 0 \wedge (a + 1) = 0$

IMP L

$green \neq red$
 $b > 0 \wedge a = 0$
 $ml_lI = green$
 $ml_lI = red \vee il_lI = red$
 $il_lI = green$
 $\vdash$
 $b > 0 \wedge (a + 1) = 0$

AND L

$green \neq red$
 $b > 0$
 $a = 0$
 $ml_lI = green$
 $ml_lI = red \vee il_lI = red$
 $il_lI = green$
 $\vdash$
 $b > 0 \wedge (a + 1) = 0$

AND R

$green \neq red$
 $b > 0$
 $a = 0$
 $ml_lI = green$
 $ml_lI = red \vee il_lI = red$
 $il_lI = green$
 $\vdash$
 $b > 0$

HYP

$green \neq red$
 $b > 0$
 $a = 0$
 $ml_lI = green$
 $ml_lI = red \vee il_lI = red$
 $il_lI = green$
 $\vdash$
 $(a + 1) = 0$

EQLR,
MON

$green \neq red$
 $ml_lI = green$
 $il_lI = red \vee il_lI = red$
 $il_lI = green$
 $\vdash$
 $(0 + 1) = 0$

ARI

$green \neq red$
 $ml_lI = green$
 $il_lI = red \vee il_lI = red$
 $il_lI = green$
 $\vdash$
 $1 = 0$

OR L

$green \neq red$
 $ml_lI = green$
 $il_lI = red$
 $1 = 0$

EQLR,
MON

$green \neq red$
 $il_lI = green$
 $1 = 0$

NOT L

$green = red$
 $il_lI = green$
 $1 \neq 0$
 $green = red$

HYP

$green \neq red$
 $ml_lI = green$
 $il_lI = red$
 $1 = 0$

EQLR,
MON

$green \neq red$
 $ml_lI = green$
 $red = green$
 $1 = 0$

NOT L

$ml_lI = green$
 $red = green$
 $1 \neq 0$
 $green = red$

HYP

4 Discharging the PO of Invariant Preservation: IL.out/inv2.3/INV (2nd Attempt)

$d \in \mathbb{N}$
 $d > 0$
 $COLOUR = \{green, red\}$
 $green \neq red$
 $n \in \mathbb{N}$
 $n \leq d$
 $a \in \mathbb{N}$
 $b \in \mathbb{N}$
 $c \in \mathbb{N}$
 $a + b + c = n$
 $a = 0 \vee c = 0$
 $ml_l \in COLOUR$
 $il_l \in COLOUR$
 $ml_l = green \Rightarrow a + b < d \wedge c = 0$
 $il_l = green \Rightarrow b > 0 \wedge a = 0$
 $ml_l = red \vee il_l = red$
 $il_l = green$
 $\vdash$
 $ml_l = green \Rightarrow a + (b - 1) < d \wedge (c + 1) = 0$

MON

$green \neq red$
 $ml_l = green \Rightarrow a + b < d \wedge c = 0$
 $ml_l = red \vee il_l = red$
 $il_l = green$
 $\vdash$
 $ml_l = green \Rightarrow a + (b - 1) < d \wedge (c + 1) = 0$

IMP_R

$green \neq red$
 $ml_l = green \Rightarrow a + b < d \wedge c = 0$
 $il_l = green$
 $ml_l = red \vee il_l = red$
 $ml_l = green$
 $\vdash$
 $a + (b - 1) < d \wedge (c + 1) = 0$

IMP_L

