EECS3342 Winter 2022
Notes on Discharging POs of Refinement
Invariant Preservation, Convergence, Deadlock Freedom
Bridge Controller: 2nd Refinement

CHEN-WEI WANG

Contents

1 Discharing the PO of Invariant Preservation: ML_out/inv2_4/INV (1st Attempt) 2

2 Discharing the PO of Invariant Preservation: IL_out/inv2_3/INV (1st Attempt) 3

3 Discharing the PO of Invariant Preservation: ML_out/inv2_4/INV (2nd Attempt) 4

4 Discharing 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)

$d \in \mathbb{N}$
$d > 0$
$COLOUR = \{green, red\}$
$green \neq red$
$n \in \mathbb{N}$
$n \leq d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \lor c = 0$
$ml\_tl \in COLOUR$
$il\_tl \in COLOUR$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$il\_tl = green \Rightarrow b > 0 \land a = 0$
$ml\_tl = green$
$\vdash$
$il\_tl = green \Rightarrow b > 0 \land (a + 1) = 0$

MON

$green \neq red$
$il\_tl = green \Rightarrow b > 0 \land a = 0$
$ml\_tl = green$
$\vdash$
$il\_tl = green \Rightarrow b > 0 \land (a + 1) = 0$

IMP_R

$green \neq red$
$il\_tl = green \Rightarrow b > 0 \land a = 0$
$ml\_tl = green$
$il\_tl = green$
$\vdash$
$b > 0 \land (a + 1) = 0$

IMP_L

$green \neq red$
$b > 0 \land a = 0$
$ml\_tl = green$
$il\_tl = green$
$\vdash$
$b > 0 \land (a + 1) = 0$

AND_L

$green \neq red$
$b > 0$
$a = 0$
$ml\_tl = green$
$il\_tl = green$
$\vdash$
$b > 0 \land (a + 1) = 0$

AND_R

Branch 1:

$green \neq red$
$b > 0$
$a = 0$
$ml\_tl = green$
$il\_tl = green$
$\vdash$
$b > 0$

HYP

Branch 2:

$green \neq red$
$b > 0$
$a = 0$
$ml\_tl = green$
$il\_tl = green$
$\vdash$
$(a + 1) = 0$

EQ_LR, MON

$green \neq red$
$ml\_tl = green$
$il\_tl = green$
$\vdash$
$(0 + 1) = 0$

ARI

$green \neq red$
$ml\_tl = green$
$il\_tl = green$
$\vdash$
$1 = 0$

??

2 Discharging the PO of Invariant Preservation: IL_out/inv2_3/INV (1st Attempt)

$d \in \mathbb{N}$
$d > 0$
$COLOUR = \{green, red\}$
$green \neq red$
$n \in \mathbb{N}$
$n \leq d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \lor c = 0$
$ml\_tl \in COLOUR$
$il\_tl \in COLOUR$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$il\_tl = green \Rightarrow b > 0 \land a = 0$
$il\_tl = green$
$\vdash$
$ml\_tl = green \Rightarrow a + (b - 1) < d \land (c + 1) = 0$

MON

$green \neq red$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$il\_tl = green$
$\vdash$
$ml\_tl = green \Rightarrow a + (b - 1) < d \land (c + 1) = 0$

IMP_R

$green \neq red$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$il\_tl = green$
$ml\_tl = green$
$\vdash$
$a + (b - 1) < d \land (c + 1) = 0$

IMP_L

$green \neq red$
$a + b < d \land c = 0$
$il\_tl = green$
$ml\_tl = green$
$\vdash$
$a + (b - 1) < d \land (c + 1) = 0$

AND_L

$green \neq red$
$a + b < d$
$c = 0$
$il\_tl = green$
$ml\_tl = green$
$\vdash$
$a + (b - 1) < d \land (c + 1) = 0$

AND_R

Branch 1:

$green \neq red$
$a + b < d$
$c = 0$
$il\_tl = green$
$ml\_tl = green$
$\vdash$
$a + (b - 1) < d$

MON

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

ARI

Branch 2:

$green \neq red$
$a + b < d$
$\mathbf{c} = \mathbf{0}$
$il\_tl = green$
$ml\_tl = green$
$\vdash$
$(c + 1) = 0$

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)

$d \in \mathbb{N}$
$d > 0$
$COLOUR = \{green, red\}$
$green \neq red$
$n \in \mathbb{N}$
$n \leq d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \lor c = 0$
$ml\_tl \in COLOUR$
$il\_tl \in COLOUR$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$il\_tl = green \Rightarrow b > 0 \land a = 0$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$il\_tl = green \Rightarrow b > 0 \land (a + 1) = 0$

MON

$green \neq red$
$il\_tl = green \Rightarrow b > 0 \land a = 0$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$il\_tl = green \Rightarrow b > 0 \land (a + 1) = 0$

IMP_R

$green \neq red$
$il\_tl = green \Rightarrow b > 0 \land a = 0$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$b > 0 \land (a + 1) = 0$

IMP_L

$green \neq red$
$b > 0 \land a = 0$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$b > 0 \land (a + 1) = 0$

AND_L

$green \neq red$
$b > 0$
$a = 0$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$b > 0 \land (a + 1) = 0$

AND_R

Branch 1:

$green \neq red$
$b > 0$
$a = 0$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$b > 0$

HYP

Branch 2:

$green \neq red$
$b > 0$
$a = 0$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$(a + 1) = 0$

EQ_LR, MON

$green \neq red$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$(0 + 1) = 0$

ARI

$green \neq red$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$1 = 0$

OR_L

Branch 2.1:

$green \neq red$
$ml\_tl = green$
$ml\_tl = red$
$il\_tl = green$
$\vdash$
$1 = 0$

EQ_LR, MON

$green \neq red$
$green = red$
$il\_tl = green$
$\vdash$
$1 = 0$

NOT_L

$green = red$
$il\_tl = green$
$1 \neq 0$
$\vdash$
$green = red$

HYP

Branch 2.2:

$green \neq red$
$ml\_tl = green$
$il\_tl = red$
$il\_tl = green$
$\vdash$
$1 = 0$

EQ_LR, MON

$green \neq red$
$ml\_tl = green$
$red = green$
$\vdash$
$1 = 0$

NOT_L

$ml\_tl = green$
$red = green1 \neq 0$
$\vdash$
$green = red$

HYP

4 Discharging the PO of Invariant Preservation: IL_out/inv2_3/INV (2nd Attempt)

$d \in \mathbb{N}$
$d > 0$
$COLOUR = \{green, red\}$
$green \neq red$
$n \in \mathbb{N}$
$n \leq d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \lor c = 0$
$ml\_tl \in COLOUR$
$il\_tl \in COLOUR$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$il\_tl = green \Rightarrow b > 0 \land a = 0$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$ml\_tl = green \Rightarrow a + (b-1) < d \land (c+1) = 0$

MON

$green \neq red$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$ml\_tl = green \Rightarrow a + (b-1) < d \land (c+1) = 0$

IMP_R

$green \neq red$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$a + (b-1) < d \land (c+1) = 0$

IMP_L

$green \neq red$
$a + b < d \land c = 0$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$a + (b-1) < d \land (c+1) = 0$

AND_L

$green \neq red$
$a + b < d$
$c = 0$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$a + (b-1) < d \land (c+1) = 0$

AND_R

Branch 1:

$green \neq red$
$a + b < d$
$c = 0$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$a + (b-1) < d$

MON

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

ARI

Branch 2:

$green \neq red$
$a + b < d$
$c = 0$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$(c+1) = 0$

EQ_LR, MON

$green \neq red$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$(0+1) = 0$

ARI

$green \neq red$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$1 = 0$

OR_L

Branch 2.1:

$green \neq red$
$il\_tl = green$
$ml\_tl = red$
$ml\_tl = green$
$\vdash$
$1 = 0$

EQ_LR, MON

$green \neq red$
$il\_tl = green$
$red = green$
$\vdash$
$1 = 0$

NOT_L

$il\_tl = green$
$red = green$
$1 \neq 0$
$\vdash$
$green = red$

HYP

Branch 2.2:

$green \neq red$
$il\_tl = green$
$il\_tl = red$
$ml\_tl = green$
$\vdash$
$1 = 0$

EQ_LR, MON

$green \neq red$
$green = red$
$ml\_tl = green$
$\vdash$
$1 = 0$

NOT_L

$green = red$
$ml\_tl = green$
$1 \neq 0$
$\vdash$
$green = red$

HYP