

EECS3342 Winter 2022
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

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

MON

$a + b + \textcolor{green}{c} = n$
 $a + b < d$
 $\textcolor{green}{c = 0}$
 \top
 $n < d$

EQ_LR, MON

$a + b + \textcolor{red}{0} = n$
 $a + b < d$
 \vdash
 $n < d$

ARI

$\textcolor{green}{a + b = n}$
 $\textcolor{green}{a + b < d}$
 \top
 $n < d$

EQ_LR, MON

$\textcolor{red}{n} < d$
 \vdash
 $n < d$

HYP

2 Discharging the PO of Guard Strengthening: ML_in/GRD

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

MON

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

OR_L

$b \in \mathbb{N}$
 $\textcolor{green}{a} + b + c = n$
 $\textcolor{red}{a} = 0$
 $c > 0$
 \vdash
 $n > 0$

EQ_LR, MON

$b \in \mathbb{N}$
 $\textcolor{red}{a} + b + c = n$
 $c > 0$
 \vdash
 $n > 0$

ARI

$b \in \mathbb{N}$
 $b + c = n$
 $c > 0$
 \vdash
 $n > 0$

ARI

$\textcolor{green}{c} \leq n$
 $\textcolor{green}{c} > 0$
 \vdash
 $n > 0$

ARI

$n > 0$
 \vdash
 $n > 0$

HYP

$b \in \mathbb{N}$
 $a + b + \textcolor{green}{c} = n$
 $\textcolor{red}{c} = 0$
 $\textcolor{green}{c} > 0$
 \vdash
 $n > 0$

EQ_LR

$b \in \mathbb{N}$
 $a + b + \textcolor{red}{c} = n$
 $\textcolor{green}{c} = 0$
 $\textcolor{red}{c} > 0$
 \vdash
 $n > 0$

EQ_LR, MON

$\textcolor{green}{0} > 0$
 \vdash
 $n > 0$

ARI

\perp
 \vdash
 $n > 0$

FALSE_L

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

MON

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

ARI

$\textcolor{green}{a + b + c = n}$
\vdash
$\textcolor{green}{a + b + c + 1 = n + 1}$

EQ_LR, MON

\vdash
$n + 1 = n + 1$

EQ

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

MON

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

OR_L

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

OR_R1

$\textcolor{green}{a = 0}$
 $c > 0$
 \top
 $a = 0$

HYP

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

EQ_LR, MON

$0 > 0$
 \top
 $a = 0 \vee (0 - 1) = 0$

ARI

\perp
 \top
 $a = 0 \vee -1 = 0$

FALSE_L