EECS3342 Winter 2023
Notes on Discharging POs of Refinement
(Guard Strengthening & Invariant Preservation)
Bridge Controller: Initial Model vs. 1st Refinement

CHEN-WEI WANG

Contents

1 Discharing the PO of Guard Strengthening: ML_out/GRD

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

MON

$$a + b + \boldsymbol{c} = n$$
$$a + b < d$$
$$\boldsymbol{c = 0}$$
$$\vdash$$
$$n < d$$

EQ_LR, MON

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

ARI

$$\boldsymbol{a + b = n}$$
$$\boldsymbol{a + b} < d$$
$$\vdash$$
$$n < d$$

EQ_LR, MON

$$\boldsymbol{n} < d$$
$$\vdash$$
$$n < d$$

HYP

2 Discharging the PO of Guard Strengthening: ML_in/GRD

Box 1 (rule **MON**):

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

MON →

Box 2 (rule **OR_L**):

$$b \in \mathbb{N}$$
$$a + b + c = n$$
$$a = 0 \lor c = 0$$
$$c > 0$$
$$\top$$
$$n > 0$$

OR_L splits into two branches.

Upper branch

EQ_LR, MON →

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

EQ_LR, MON → (rule **ARI**)

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

ARI →

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

ARI →

$$c \leq n$$
$$c > 0$$
$$\top$$
$$n > 0$$

ARI → (rule **HYP**)

$$n > 0$$
$$\top$$
$$n > 0$$

Lower branch

EQ_LR →

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

EQ_LR, MON →

$$b \in \mathbb{N}$$
$$a + b + 0 = n$$
$$0 > 0$$
$$\top$$
$$n > 0$$

ARI → (rule **FALSE_L**)

$$0 > 0$$
$$\top$$
$$n > 0$$

FALSE_L →

$$\bot$$
$$\top$$
$$n > 0$$
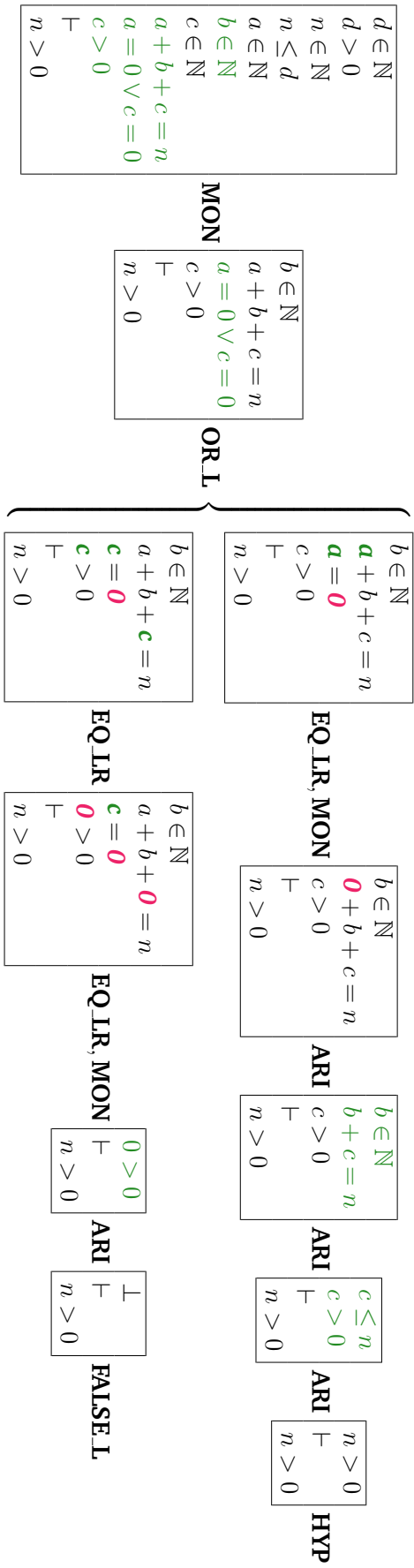
3 Discharing the PO of Invariant Preservation: ML_out/inv1_4/INV

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

MON

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

ARI

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

EQ_LR, MON

$$\vdash$$
$$n + 1 = n + 1$$

EQ

4 Discharing the PO of Invariant Preservation: ML_in/inv1_5/INV

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

MON

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

OR_L

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

OR_R1

$\boldsymbol{a = 0}$
$c > 0$
$\top$
$a = 0$

HYP

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

EQ_LR, MON

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

ARI

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

FALSE_L