EECS3342 Winter 2023
Notes on Discharging POs of Refinement Invariant Preservation
File Transfer Protocol: 1st Refinement

CHEN-WEI WANG

Contents

1 Discharing the PO of Invariant Preservation: receive/inv1_1/INV

$$
\begin{array}{l}
n > 0 \\
f \in 1 \mathinner{..} n \rightarrow D \\
BOOLEAN = \{TRUE, FALSE\} \\
g \in 1 \mathinner{..} n \nrightarrow D \\
b \in BOOLEAN \\
b = FALSE \Rightarrow g = \varnothing \\
b = TRUE \Rightarrow g = f \\
r \in 1 \mathinner{..} n+1 \\
h = (1 \mathinner{..} r-1) \lhd f \\
b = TRUE \Rightarrow r = n+1 \\
r \leq n \\
\vdash \\
(r+1) \in 1 \mathinner{..} n+1
\end{array}
$$

MON

$$
\begin{array}{l}
r \in 1 \mathinner{..} n+1 \\
r \leq n \\
\vdash \\
(r+1) \in 1 \mathinner{..} n+1
\end{array}
$$

ARI

$$
\begin{array}{l}
1 \leq r \wedge r \leq n+1 \\
r \leq n \\
\vdash \\
\quad 1 \leq (r+1) \\
\wedge \quad (r+1) \leq n+1
\end{array}
$$

AND_L

$$
\begin{array}{l}
1 \leq r \\
r \leq n+1 \\
r \leq n \\
\vdash \\
\quad 1 \leq (r+1) \\
\wedge \quad (r+1) \leq n+1
\end{array}
$$

AND_R

$$
\begin{array}{l}
1 \leq r \\
r \leq n+1 \\
\vdash \\
1 \leq (r+1)
\end{array}
$$

MON

$$
\begin{array}{l}
1 \leq r \\
\vdash \\
1 \leq (r+1)
\end{array}
$$

ARI

$$
\begin{array}{l}
1 \leq r \\
r \leq n+1 \\
r \leq n \\
\vdash \\
(r+1) \leq n+1
\end{array}
$$

MON

$$
\begin{array}{l}
r \leq n \\
\vdash \\
(r+1) \leq n+1
\end{array}
$$

ARI

$$
\begin{array}{l}
r \leq n \\
r \leq n
\end{array}
\quad \vdash \quad
r \leq n
$$

HYP

2 Discharing the PO of Invariant Preservation: receive/inv1_2/INV

$$
\begin{array}{l}
n > 0 \\
f \in 1 \mathinner{..} n \to D \\
BOOLEAN = \{TRUE, FALSE\} \\
g \in 1 \mathinner{..} n \nrightarrow D \\
b \in BOOLEAN \\
b = FALSE \Rightarrow g = \varnothing \\
b = TRUE \Rightarrow g = f \\
r \in 1 \mathinner{..} n+1 \\
h = (1 \mathinner{..} r-1) \lhd f \\
b = TRUE \Rightarrow r = n+1 \\
r \leq n \\
\vdash \\
h \cup \{(r, f(r))\} = (1 \mathinner{..} (r+1)-1) \lhd f
\end{array}
$$

MON

$$
\begin{array}{l}
f \in 1 \mathinner{..} n \to D \\
r \in 1 \mathinner{..} n+1 \\
h = (1 \mathinner{..} r-1) \lhd f \\
r \leq n \\
\vdash \\
h \cup \{(r, f(r))\} = (1 \mathinner{..} (r+1)-1) \lhd f
\end{array}
$$

ARI

$$
\begin{array}{l}
f \in 1 \mathinner{..} n \to D \\
1 \leq r \\
h = (1 \mathinner{..} r-1) \lhd f \\
r \leq n \\
\vdash \\
h \cup \{(r, f(r))\} = (1 \mathinner{..} (r+1)-1) \lhd f
\end{array}
$$

EQ_LR, MON, ARI

$$
\begin{array}{l}
f \in 1 \mathinner{..} n \to D \\
1 \leq r \\
r \leq n \\
\vdash \\
(1 \mathinner{..} r-1) \lhd f \cup \{(r, f(r))\} = (1 \mathinner{..} r) \lhd f
\end{array}
$$

ARI

3 Discharing the PO of Invariant Preservation: receive/inv1_3/INV

$$
\begin{array}{l}
n > 0 \\
f \in 1 \mathinner{..} n \rightarrow D \\
BOOLEAN = \{TRUE, FALSE\} \\
g \in 1 \mathinner{..} n \nrightarrow D \\
b \in BOOLEAN \\
b = FALSE \Rightarrow g = \varnothing \\
b = TRUE \Rightarrow g = f \\
r \in 1 \mathinner{..} n+1 \\
h = (1 \mathinner{..} r-1) \lhd f \\
b = TRUE \Rightarrow r = n+1 \\
r \leq n \\
\vdash \\
b = TRUE \Rightarrow (r+1) = n+1
\end{array}
$$

MON

$$
\begin{array}{l}
b = TRUE \Rightarrow r = n+1 \\
r \leq n \\
\vdash \\
b = TRUE \Rightarrow (r+1) = n+1
\end{array}
$$

IMP_R

$$
\begin{array}{l}
b = TRUE \Rightarrow r = n+1 \\
r \leq n \\
b = TRUE \\
\vdash \\
(r+1) = n+1
\end{array}
$$

IMP_L

$$
\begin{array}{l}
\boldsymbol{r = n+1} \\
\boldsymbol{r} \leq n \\
b = TRUE \\
\vdash \\
(\boldsymbol{r}+1) = n+1
\end{array}
$$

EQ_LR, MON

$$
\begin{array}{l}
n+1 \leq n \\
b = TRUE \\
\vdash \\
((n+1)+1) = n+1
\end{array}
$$

ARI, MON

$$
\begin{array}{l}
\bot \\
\vdash \\
((n+1)+1) = n+1
\end{array}
$$

FALSE_L