# AR TUTORIAL 7 - Hoare Logic

EXERCISE ONE: Construct the Natural Deduction proof for the following Hoare Logic triple (from the factorial example from lecture) on paper:

$\{Y=1 \wedge Z=0\}$ WHILE $Z \neq X$ DO $Z := Z+1; Y := Y \times Z$ OD $\{Y=X!\}$

You may use any of the FOL natural deduction rules and the Hoare Logic rules. Additionally, you may use the following 4 lemmas:

$$\frac{\neg\neg X}{X}\ \text{notnotD} \qquad \frac{b=a}{a=b}\ \text{sym} \qquad \frac{}{0!=1}\ \text{fact\_0}$$

$$\frac{}{X! * (X+1) = (X+1)!}\ \text{factplus\_1} \qquad \frac{s=t \quad Ps}{Pt}\ \text{subst}$$

(1)

$$\dfrac{\dfrac{\dfrac{[Y=Z! \wedge \neg Z \neq X]_1}{Y=X!}\ \text{conjE}_2 \qquad \dfrac{\dfrac{[\neg Z \neq X]_2}{Z=X}\ \text{notnotD} \qquad [Y=Z!]_2}{Y=X!}\ \text{subst}}{Y=Z! \wedge \neg Z \neq X \rightarrow Y=X!}\ \text{impI}_1$$

(2)

$$\dfrac{\dfrac{\dfrac{\dfrac{}{0!=1}\ \text{fact\_0}}{1=0!} \qquad \dfrac{[Z=0]_4}{0=Z}\ \text{sym}}{1=Z!}\ \text{subst} \qquad [Y=1]_4}{Y=Z!}\ \text{subst} \qquad [Y=1 \wedge Z=0]_3}{Y=Z!}\ \text{conjE}_4$$

$$\frac{Y=Z!}{Y=1 \wedge Z=0 \rightarrow Y=Z!}\ \text{impI}_3$$

(3)

$$\dfrac{\dfrac{\dfrac{\dfrac{[Y=Z! \wedge Z \neq X]_5}{Y=Z!}\ \text{conjunct1}}{Z!=Y}\ \text{sym} \qquad \dfrac{}{Z! \times (Z+1) = (Z+1)!}\ \text{fact\_plus\_1}}{Y \times (Z+1) = (Z+1)!}\ \text{subst}}{Y=Z! \wedge Z \neq X \rightarrow Y \times (Z+1) = (Z+1)!}\ \text{impI}_5$$

(4)

(3)

$Y = Z! \wedge Z \neq X \rightarrow Y \times (Z+1) = (Z+1)!$

$\{Y \times (Z+1) = (Z+1)!\}\ Z := Z+1 \{Y \times Z = Z!\}$ ASSIGN

$\{Y = Z! \wedge Z \neq X\}\ Z := Z+1 \{Y \times Z = Z!\}$ PS

$\{Y \times Z = Z!\}\ Y := Y \times Z \{Y = Z!\}$ ASSIGN

$\{Y = Z! \wedge Z \neq X\}\ Z := Z+1; Y := Y \times Z \{Y = Z!\}$ SEQ

(5)

(2)

$Y = 1 \wedge Z = 0 \rightarrow Y = Z!$

(4)

$\{Y = Z! \wedge Z \neq X\}\ Z := Z+1; Y := Y \times Z \{Y = Z!\}$

$\{Y = Z!\}$ WHILE $Z \neq X$ DO $Z := Z+1; Y := Y \times Z$ OD $\{Y = Z!\} \wedge \neg Z \neq X$ WHILE

$\{Y = 1 \wedge Z = 0\}$ WHILE $Z \neq X$ DO $Z := Z+1; Y := Y \times Z$ OD $\{Y = Z!\} \wedge \neg Z \neq X$ PS

(1)

$Y = Z! \wedge \neg Z \neq X \rightarrow Y = X!$

$\{Y = 1 \wedge Z = 0\}$ WHILE $Z \neq X$ DO $Z := Z+1; Y := Y \times Z$ OD $\{Y = X!\}$ PW

## SOLUTION (from tutorial discussion)

Post-condition weakening: $\dfrac{\{P\}\ y\ \{Q'\}}{\{P\}\ y\ \{Q\}}\ Q' \to Q$

$y = z! \wedge \neg(z \neq x) \to y = x!$

Pre-condition strengthening: $\dfrac{P \to P' \quad \{P'\}\ y\ \{Q\}}{\{P\}\ y\ \{Q\}}$

$(y = 1 \wedge z = 0) \to y = z!$

WHILE → $\dfrac{\{P \wedge S\}\ y\ \{P\}}{\{P\}\ \text{WHILE } S \text{ DO } C \text{ OD } \{P \wedge \neg S\}\ y}$

Need to find invariant $P$ such that

$\{P \wedge z \neq x\}\ y\ z := z+1;\ y := y \times z\ \{P\}\ y$ → because $y = z! \wedge z \neq x \to y \times (z+1) = (z+1)!$

$y = 1 \wedge z = 0 \to P$ ⟶ $0! = 1$

$P \wedge \neg(z \neq x) \to y = x!$ ⟶ because $\neg(z \neq x) \leftrightarrow z = x$

answer: $y = z!$

$$\dfrac{\dfrac{\{y \times (z+1) = (z+1)!\}\ y\ z := z+1\ \{y \times z = z!\}\ y \qquad \{y \times z = z!\}\ y\ y := y \times z\ \{y = z!\}\ y}{\{y \times (z+1) = (z+1)!\}\ y\ z := z+1;\ y := y \times z\ \{y = z!\}\ y}}{\vdash \{y = 1 \wedge z = 0\}\ y\ \text{WHILE } z \neq x \text{ DO } z := z+1;\ y := y \times z \text{ OD } \{y = x!\}\ y}$$

$P \to$ holds at each iteration

$\{P \wedge \neg z \neq x\}\ y$

$$\dfrac{\vdash \{y = 1 \wedge z = 0\}\ y \Rightarrow R \qquad \vdash \{R \wedge (z \neq x)\}\ y\ z := z+1\ \{R\}\ y \qquad \vdash R \wedge \neg(z \neq x) \Rightarrow [(x \times z)/z]}{\dfrac{\vdash \{y = 1 \wedge z = 0\}\ y\ \text{WHILE } z \neq x \text{ DO } z := z+1\ \{y = x![(y \times z)/y]\}\ y}{\vdash \{y = 1 \wedge z = 0\}\ y\ \text{WHILE } z \neq x \text{ DO } z := z+1;\ y := y \times z \text{ OD } \{y = x!\}\ y}\ \text{seq}}$$

P — S — C — R

P — C — V — E — Q