# Solutions for Tutorial 6/7: Rewrite Rules, Hoare Logic and Induction

## Exercise 1: Critical Pairs (Past exam question)

Recall from the lectures that for rewrite rules $L1 \Rightarrow R_1$ and $L2 \Rightarrow R_2$, a critical pair can be defined as:

$$\langle R_1[\theta], L_1[\theta]/\{R_2[\theta]/s\}\rangle$$

where $\theta = mgu$ of $s$ (subpart of $L_1$) and $L_2$.

Now if we take:

$$\overbrace{\underbrace{(u+v)}_{s} + w}^{L_1} \Rightarrow \overbrace{u + (v + w)}^{R_1}$$

$$\overbrace{s(x) + y}^{L_2} \Rightarrow \overbrace{x + s(y)}^{R_2}$$

Then $\theta = [s(x)/u, y/v]$, so the critical pair is given by

$$\langle\ s(x) + (y + w), (x + s(y)) + w\rangle$$

More concisely: The expression $s(x)+y$ unifies with $u+v$ with common instance $s(x)+y$. $(s(x)+y)+w$ can be rewritten to either $(x+s(y))+w$ or $s(x)+(y+w)$. So the critical pair is:

$$\langle\ s(x) + (y + w), (x + s(y)) + w\rangle$$

## Exercise 2: Confluence (Past exam question)

Two examples of critical pairs that are not joinable are: 1) starting from $(X\cdot 0)\cdot Z$ we can get the critical pair $\langle X \cdot (0 \cdot Z), X \cdot Z\rangle$; and 2) starting from $(X \cdot i(X)) \cdot Z$ we can get the critical pair $\langle 0 \cdot Z, X \cdot (i(X) \cdot Z)\rangle$. To get full marks, you must mention that the critical pair is not joinable (or "conflatable").

## Exercise 3: Induction

1. An appropriate induction rule is:

$$\frac{\Gamma \vdash P(\texttt{LEAF}\ x) \quad \Gamma, P(x_1), P(x_2) \vdash P(\texttt{NODE}\ a\ x_1\ x_2)}{\Gamma \vdash \forall t. P(t)}$$

2. An Isabelle definition:

```
primrec MIRROR :: "'a TREE => 'a TREE" where
  "MIRROR (LEAF x) = LEAF x"
| "MIRROR (NODE x l r) = NODE x (MIRROR r) (MIRROR l)"
```

3. See theory file for proof of theorem.

**Exercise 4: Pen-and-Paper Hoare Logic Proof**

# Available lemmas/rules:

$$\frac{\neg\neg X}{X}\ \mathit{notnotD} \qquad \frac{b = a}{a = b}\ \mathit{sym} \qquad \frac{}{0! = 1}\ \mathit{fact\_0} \qquad \frac{}{x! \times (x+1) = (x+1)!}\ \mathit{fact\_plus\_1}$$

# Factorial proof:

$$\dfrac{\dfrac{[Y = Z! \wedge \neg Z \neq X]_1 \qquad \dfrac{\dfrac{[\neg Z \neq X]_2}{Z = X}\ \mathit{notnotD} \qquad [Y = Z!]_2}{Y = X!}\ \mathit{subst}}{Y = X!}\ \mathit{conjE}_2}{Y = Z! \wedge \neg Z \neq X \rightarrow Y = X!}\ \mathit{impI}_1 \tag{1}$$

$$\dfrac{\dfrac{[Y = 1 \wedge Z = 0]_3 \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{0! = 1}\ \mathit{fact\_0}}{1 = 0!}\ \mathit{sym} \qquad \dfrac{[Z = 0]_4}{0 = Z}\ \mathit{sym}}{1 = Z!}\ \mathit{subst} \qquad [Y = 1]_4}{Y = Z!}\ \mathit{subst}}{Y = Z!}\ \mathit{conjE}_4}{Y = 1 \wedge Z = 0 \rightarrow Y = Z!}\ \mathit{impI}_3 \tag{2}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{[Y = Z! \wedge Z \neq X]_5}{Y = Z!}\ \mathit{conjunct1}}{Z! = Y}\ \mathit{sym} \qquad \dfrac{}{Z! \times (Z+1) = (Z+1)!}\ \mathit{fact\_plus\_1}}{Y \times (Z+1) = (Z+1)!}\ \mathit{subst}}{Y = Z! \wedge Z \neq X \rightarrow Y \times (Z+1) = (Z+1)!}\ \mathit{impI}_5 \tag{3}$$

$$\dfrac{\dfrac{\dfrac{(3)}{Y = Z! \land Z \neq X \to Y \times (Z+1) = (Z+1)!} \quad \dfrac{}{\{Y \times (Z+1) = (Z+1)!\} Z := Z+1 \{Y \times Z = Z!\}}\,\mathit{ASSIGN}}{\{Y = Z! \land Z \neq X\} Z := Z+1 \{Y \times Z = Z!\}}\,\mathit{PS} \quad \dfrac{}{\{Y \times Z = Z!\} Y := Y \times Z \{Y = Z!\}}\,\mathit{ASSIGN}}{\{Y = Z! \land Z \neq X\} Z := Z+1; Y := Y \times Z \{Y = Z!\}}\,\mathit{SEQ}$$

(4)

$$\dfrac{\dfrac{\dfrac{(2)}{Y = 1 \land Z = 0 \to Y = Z!} \quad \dfrac{\dfrac{(4)}{\{Y = Z! \land Z \neq X\} Z := Z+1; Y := Y \times Z \{Y = Z!\}}}{\{Y = Z!\}\,\mathtt{WHILE}\ Z \neq X\ \mathtt{DO}\ Z := Z+1; Y := Y \times Z\ \mathtt{OD}\,\{Y = Z! \land \neg Z \neq X\}}\,\mathit{WHILE}}{\{Y = 1 \land Z = 0\}\,\mathtt{WHILE}\ Z \neq X\ \mathtt{DO}\ Z := Z+1; Y := Y \times Z\ \mathtt{OD}\,\{Y = Z! \land \neg Z \neq X\}}\,\mathit{PS} \quad \dfrac{(1)}{Y = Z! \land \neg Z \neq X \to Y = X!}}{\{Y = 1 \land Z = 0\}\,\mathtt{WHILE}\ Z \neq X\ \mathtt{DO}\ Z := Z+1; Y := Y \times Z\ \mathtt{OD}\,\{Y = X!\}}\,\mathit{PW}$$

(5)

## Exercise 5: Introduction to Hoare Logic in Isabelle

See Isabelle theory file.