COMP4161 S2/2016
Advanced Topics in Software Verification

Assignment 1

This assignment starts on Mon, 2016-08-08 and is due on Mon, 2016-08-15, 23:59h. We will accept plain text (.txt) files, PDF (.pdf) files, and Isabelle theory (.thy) files.

The assignment is take-home. This does NOT mean you can work in groups. Each submission is personal. For more information, see the plagiarism policy: https://student.unsw.edu.au/plagiarism

Submit using `give` on a CSE machine:

```
give cs4161 a1 files ...
```

For example:

```
give cs4161 a1 a1.thy a1.pdf
```

1 Types (15 marks)

Construct a type derivation tree for the term $\lambda a\ b\ c.\ a\ (x\ b\ b)\ (c\ b)$.

Each node of the tree should correspond to the application of a *single* typing rule, indicating which typing rule is used at each step.

Under which contexts is the term type correct?

2 λ-Calculus (20 marks)

Recall the encoding of booleans and booleans operations in lambda calculus seen in the lecture:

$$\begin{array}{lcl} \texttt{true} & \equiv & \lambda x\ y.\ x \\ \texttt{false} & \equiv & \lambda x\ y.\ y \\ \texttt{if} & \equiv & \lambda z\ x\ y.\ z\ x\ y \\ \texttt{or} & \equiv & \lambda x\ y.\ \texttt{if}\ x\ \texttt{true}\ y \end{array}$$

(a) Show that the β normal form for `or true false` is `true`. Justify your answer by providing the β reduction steps leading from the term to its normal form. Each step should only reduce *one* redex (i.e. one reduction per step). Ideally, you would underline the redex being reduced. (10 marks)

(b) Provide a type for `true`. Justify your answer by providing a derivation tree. (5 marks)

(c) What is a type of `or true false`? Justify your answer. (5 marks)

3 Propositional Logic (25 marks)

Prove each of the following statements, using only the proof methods `rule`, `erule`, `assumption`, `frule`, and `drule`; and using only the proof rules `impI`, `impE`, `conjI`, `conjE`, `disjI1`, `disjI2`, `disjE`, `notI`, `notE`, `iffI`, `iffE`, `iffD1`, `iffD2`, `ccontr`, `classical`, `FalseE`, `TrueI`, `conjunct1`, `conjunct2`, and `mp`. You do not need to use all of these methods and rules.

(a) $A \wedge B \longrightarrow B$ (2 marks)

(b) $(P \vee P) = P$ (3 marks)

(c) $\neg \neg P \longrightarrow P$ (3 marks)

(d) $(A \wedge B \longrightarrow C) = (A \longrightarrow B \longrightarrow C)$ (5 marks)

(e) $(\neg x) = (x = \mathit{False})$ (5 marks)

(f) $(a \longrightarrow b) = (\neg (a \wedge \neg b))$ (5 marks)

List the statements above that are provable only in a classical logic. (2 marks)

4 Higher-Order Logic (40 marks)

Prove each of the following statements, using only the proof methods and rules from Question 3 plus you may also use the additional methods `rule_tac`, `erule_tac`, `drule_tac`, `frule_tac`, `case_tac`, and `rename_tac`, and the additional rules `allI`, `allE`, `exI`, `exE`, and `spec`. You may use rules proved in earlier parts of the question when proving later parts.

(a) $(\forall x\, y.\ R\ x\ y) \longrightarrow (\forall y\, x.\ R\ x\ y)$ (3 marks)

(b) $(\exists x.\ P\ x \wedge Q\ x) \longrightarrow (\exists x.\ P\ x) \wedge (\exists x.\ Q\ x)$ (3 marks)

(c) $\mathit{False} = (\forall P.\ P)$ (4 marks)

(d) $\exists R.\ (\forall x.\ \exists y.\ R\ x\ y) \wedge \neg (\exists y.\ \forall x.\ R\ x\ y)$ (6 marks)

(e) $\forall x.\ \neg\ R\ x \longrightarrow RM\ x \Longrightarrow \forall x.\ \neg\ RM\ x \longrightarrow R\ x$ (6 marks)

(f) $[\![\forall x.\ \neg\ R\ x \longrightarrow R\ (M\ x);\ \exists x.\ R\ x]\!] \Longrightarrow \exists x.\ R\ x \wedge R\ (M\ (M\ x))$
(8 marks)

Formalise and prove the following statement using only the proof methods and rules as earlier in this question. (10 marks)

> If every poor person has a rich mother, then there is a rich person with a rich grandmother.