COMP4161 S2/2015
Advanced Topics in Software Verification

Assignment 1

This assignment starts on Tue, 2015-08-11 and is due on Tue, 2015-08-18, 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 λ-Calculus (30 marks)

(a) Underline the free variables in the term: $(\lambda z.\ (\lambda x\ y.\ y)\ (\lambda a.\ a\ x\ z))$ (2 marks)

(b) β-reduce the following term to its normal form:
$(\lambda x\ y.\ x)\ ((\lambda z.\ z)\ y)$ (8 marks)

(c) Write down the (most general) type of the following term:
$(\lambda x\ y.\ x)\ (\lambda y.\ y)$ (5 marks)

(d) Give a pen-and-paper proof of your answer to (c). (13 marks)

(e) For the term $(\lambda x\ y.\ x)\ (\lambda y.\ y)$, write down the type of the following sub-term: $(\lambda x\ y.\ x)$ – that is, the type that the sub-term has within the larger term. (2 marks)

2 Higher-Order Unification (10 marks)

Find a unifier (substitution) for the schematic variables in the following term so that its left- and right-hand sides are $\alpha\beta\eta$-equivalent. Justify your answer by showing that the two sides $\alpha\beta\eta$-reduce to the same term.
$(\lambda y\ x.\ ?H\ x\ y) =_{\alpha\beta\eta} (\lambda x\ y.\ ?G\ (y\ x))$ (10 marks)

3 Propositional Logic (25 marks)

Prove each of the following statements, using only the proof methods `rule`, `erule`, `case_tac` and `assumption`; and using only the proof rules `impI`, `impE`, `conjI`, `conjE`, `disjI1`, `disjI2`, `disjE`, `notI`, `notE`, `iffI`, `iffE`, `ccontr`, `classical`, `FalseE` and `TrueI`.

(a) $B \longrightarrow B \vee A$ (3 marks)

(b) $(A = \mathit{True}) = A$ (5 marks)

(c) $(A = \mathit{False}) = (\neg\ A)$ (6 marks)

(d) $P \longrightarrow \neg\ \neg\ P$ (4 marks)

(e) $\neg\ \neg\ P \longrightarrow P$ (5 marks)

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

4 Higher Order Logic (35 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` and `drule_tac`, and the additional rules `allI`, `allE`, `exI`, `exE`, `iffD1`, `iffD2`, `spec`.

(a) $(\forall x.\ P\ x) \vee (\forall x.\ Q\ x) \longrightarrow (\forall x.\ P\ x \vee Q\ x)$ (4 marks)

(b) $(\forall P.\ P) = \mathit{False}$ (3 marks)

(c) $(\forall x.\ Q\ x = P\ x) \wedge ((\exists x.\ P\ x) \longrightarrow C) \wedge (\exists x.\ Q\ x) \longrightarrow C$ (5 marks)

(d) $\forall x.\ \neg\ R\ x \longrightarrow R\ (M\ x) \Longrightarrow \forall x.\ \neg\ R\ (M\ x) \longrightarrow R\ x$ (5 marks)

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