COMP4161 S2/2017
Advanced Topics in Software Verification

Assignment 1

This assignment starts on Thu, 2017-08-03 and is due on Fri, 2017-08-11, 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 (25 marks)

1. Construct a type derivation tree for the term $\lambda x\ y\ z.\ y\ (a\ y\ z)\ (x\ z)$.

   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? (12 marks)

2. Find a term that has type $('b \Rightarrow 'c) \Rightarrow ('a \Rightarrow 'b) \Rightarrow 'a \Rightarrow 'c$.
   Give a type derivation tree. (10 marks)

3. Is there a term in simply-typed lambda calculus that has the type $(('a \Rightarrow 'b) \Rightarrow 'a) \Rightarrow 'a$?
   If yes, give the term, if no, describe why not. (3 marks)

2 λ-Calculus (30 marks)

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

`true`	$\equiv$	$\lambda x\ y.\ x$
`false`	$\equiv$	$\lambda x\ y.\ y$
`if`	$\equiv$	$\lambda z\ x\ y.\ z\ x\ y$
`or`	$\equiv$	$\lambda x\ y.$ `if` x `true` y
`and`	$\equiv$	$\lambda x\ y.$ `if` $x\ y$ `false`

1. Show that the β normal form for `and false true` is `false`. Justify your answer by providing the β reduction and definition-unfolding 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)

2. Provide the β-normal forms for `and x x` and `or x x`. Under which conditions does `and x x` $=_\beta$ `or x x` hold? (10 marks)

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

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

3 Propositional Logic (45 marks)

Prove each of the following statements, using only the proof methods `rule`, `erule`, `assumption`, `frule`, `drule`, and `cases`; 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) $\neg\neg P \longrightarrow P$ (3 marks)

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

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

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

(f) $(A \longrightarrow A) = Q \Longrightarrow Q \vee B$ (5 marks)

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

(h) $(P \longrightarrow Q) = (\neg P \vee Q)$ (5 marks)

(i) $(P \vee P \wedge Q) = (P \wedge (P \vee Q))$ (5 marks)

(j) $\neg (\neg (\neg P \vee Q) \vee P) \vee P \Longrightarrow P \vee \neg P$ (5 marks)
Do not use `cases`, `ccontr`, `classical` for (j).

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