Advanced Topics in Formal Methods and Prog. Languages
– Software Verification with Isabelle/HOL –

Assignment 1

ver 1.01

Submission Guidelines

- Due time: Aug 16, 2024, 6pm (Canberra Time)
- Submit via Wattle.
- Accepted formats are plain text (.txt) files, PDF (.pdf) files, and Isabelle theory (.thy) files.
- Scans of hand-written text are fine, as long as they are readable and neat.
- Isabelle files should be executable (a template is provided on the course webpage).
- Please read and sign the declaration on the last page and attach a copy to your submission.
- **No late submission, deadline is strict**

Exercise 1 (λ-Calculus) (16 Marks)

(a) Simplify the term $(x\ y)\ (\lambda x.(\lambda y.(\lambda z.(z\ (x\ y)))))$ syntactically by applying the syntactic conventions and rules. Justify your answer. (2 marks)

(b) Restore the omitted parentheses in the term $x\ (\lambda x\ y.\ x\ (y\ z)\ (x\ y))\ (\lambda y.\ y\ z)$. Make sure you do not change the term structure. (2 marks)

(c) Find the normal form of $(\lambda f.\ \lambda x.\ f\ (f\ (f\ x)))\ (\lambda g.\ \lambda y.\ g\ (g\ y))$. Justify your answer by showing the reduction sequence. Each step in the reduction sequence should be a single β-reduction step. Underline the redex being reduced for each step. (6 marks)

(d) Recall the encoding of natural numbers in lambda calculus (Church Numerals):

$$
\begin{aligned}
0 &\equiv \lambda f\ x.\ x \\
1 &\equiv \lambda f\ x.\ f\ x \\
2 &\equiv \lambda f\ x.\ f\ (f\ x) \\
3 &\equiv \lambda f\ x.\ f\ (f\ (f\ x)) \\
&\dots
\end{aligned}
$$

Define exp where $\mathit{exp}\ m\ n$ β-reduces to the Church Numeral representing m^n. Provide a justification of your answer. (6 marks)

Exercise 2 (Types) (20 Marks)

(a) Provide the most general type for the term $\lambda a\ b.\ a\ (c\ b)\ b$. Show a type derivation tree to justify your answer. Each node of the tree should correspond to the application of a single typing rule, and be labeled with the typing rule used. Under which contexts is the term type correct? (5 marks)

(b) Find a closed lambda term that has the following type:

$$('a \Rightarrow 'b) \Rightarrow 'a \Rightarrow ('a \Rightarrow 'b \Rightarrow 'c) \Rightarrow 'c$$

You don't need to provide a type derivation, but provide a short explanation. (4 marks)

(c) Explain why $\lambda x.\ x\ x$ is not typable. (3 marks)

(d) Find the normal form of $(\lambda x\ y.\ y)\ (\lambda z.\ z\ z)$ and give it a type. (3 marks)

(e) Is $(\lambda x\ y.\ y)\ (\lambda z.\ z\ z)$ typable? Compare this situation with the Subject Reduction that you learned in the lecture. (5 marks)

Exercise 3 (Propositional Logic) (29 Marks)

Prove each of the following statements, using only the proof methods: `rule`, `erule`, `assumption`, `cases`, `frule`, `drule`, `rule_tac`, `erule_tac`, `frule_tac`, `drule_tac`, `rename_tac`, and `case_tac`; 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) $A \longrightarrow \neg\neg A$ (3 marks)

(b) $\neg\neg\neg A \longrightarrow \neg A$ (3 marks)

(c) $\neg\neg A \longrightarrow A$ (4 marks)

(d) $\neg(A \wedge B) \longrightarrow \neg A \vee \neg B$ (4 marks)

(e) $(A \longrightarrow B) \longrightarrow \neg A \vee B$ (4 marks)

(f) $(\neg A \wedge \neg B) = (\neg(A \vee B))$ (6 marks)

(g) $(A \longrightarrow B) \longrightarrow ((B \longrightarrow C) \longrightarrow A) \longrightarrow B$ (5 marks)

Exercise 4 (Higher-Order Logic) (35 Marks)

Prove each of the following statements, using only the proof methods and proof rules stated in the previous question, plus any of the following proof rules: `allI`, `allE`, `exI`, and `exE`. You do not need to use all of these methods and rules. You may use rules proved in earlier parts of the question when proving later parts.

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

(b) $((\exists x.\ P\ x) \longrightarrow Q) = (\forall x.\ P\ x \longrightarrow Q)$ (6 marks)

(c) $(\forall x.\ P\ x) = (\nexists x.\ \neg P\ x)$ (6 marks)

(d) $(\forall x.\ P\ x \wedge Q\ x) \longrightarrow (\forall x.\ P\ x) \wedge (\forall x.\ Q\ x)$ (6 marks)

(e) $(\exists x.\ P\ x \vee Q\ x) \longrightarrow (\exists x.\ P\ x) \vee (\exists x.\ Q\ x)$ (6 marks)

(f) $(\forall x\ y.\ A\ y \vee B\ x) \longrightarrow (\forall x.\ B\ x) \vee (\forall y.\ A\ y)$ (7 marks)

Academic Integrity

I declare that this work upholds the principles of academic integrity, as defined in the University Academic Misconduct Rule; is entirely my own work, with only the exceptions listed; is produced for the purposes of this assessment task and has not been submitted for assessment in any other context, except where authorised in writing by the course convener; gives appropriate acknowledgement of the ideas, scholarship and intellectual property of others insofar as these have been used; in no part involves copying, cheating, collusion, fabrication, plagiarism or recycling.

____________________	____________________
Date	Signature