

COMP 4161 S2/08
Advanced Topics in Software Verification

Exam

This take-home exam starts on Wed, 29.10.2008, 0:00am and is due on Wed, 29.10.2008, 23:59. Please submit electronically to `gerwin.klein@nicta.com.au`. Accepted formats are plain text, Isabelle theory files and pdf documents.

1 Lambda Calculus (25 marks)

- (a) Do the following lambda terms have a $\beta\eta$ normal form? What is it? If it exists, provide a derivation.

(i) $(\lambda z x y. z x y) (\lambda x y. x) x (f x)$

(ii) $(\lambda x f. f (x x f)) (\lambda x f. f (x x f)) (\lambda f x. x)$

- (b) Answer the following for each term in question (a):
Does the term have a type? What is it?
Does its $\beta\eta$ reduct (if it exists) have the same type?

2 Balanced Parentheses (25 marks)

Define and prove the following in Isabelle.

- (a) Use an inductive set to define the set of strings over the alphabet of parentheses $\{L, R\}$ that is described by the following grammar:

$$S := \epsilon \mid L S R \mid S S$$

Prove 2 small test cases to gain confidence in the definition.

- (b) Use `fun/fundef` to define a function `is_bal` that counts opening and closing parentheses from left to right and returns true if they are balanced and false if they are not. For example `LRLRR` is balanced, `LLR` is not.

Prove 4 small test cases to gain confidence in the definition.

- (c) Show $xs \in S \implies is_bal\ xs\ 0$ (You will need to prove intermediate lemmas.)
(d) Show $is_bal\ xs\ 0 \implies xs \in S$ (Since this direction is harder, some intermediate lemma statements are provided in `Exam.thy`. You can of course use and prove different ones as well.)

3 Hoare Logic (25 marks)

Given the following program on natural numbers:

```
n := 0; m := 0; k := 0;
while k < a do
  n := n + 1;
  k := k + m + 1;
  m := m + 2
od
```

- What does the program compute, i.e. what is the relationship between the result value of n and the input a ?
- What is the invariant for the loop? Trace a few example computations in your favourite programming language to discover the relationship between the variables.
- State the property of (a) as a Hoare triple (you may need to reformulate it slightly), annotate the program with the above invariant and prove the Hoare triple.

4 Calculational Reasoning (25 marks)

Show the following group lemmas (you may need intermediate lemmas):

- The left-one is also a right-one: $x \cdot 1 = x$
- Unique division: $\exists!x. a \cdot x = b$
- Cancellation on left: $a \cdot x = a \cdot y \implies x = y$

You can assume the following group axioms provided in file `Exam.thy` on the exam web page.

```
assoc:    (x · y) · z = x · (y · z)
left_inv:  inv x · x = 1
left_one:  1 · x = x
```

Use the theorem search function to find the definition and rules for the $\exists!x. P x$ operator (there exists exactly one x such that $P x$).

You can use the locale feature as in `Exam.thy` to refer to the group axioms. You can also state them explicitly as assumptions on your lemmas if you prefer that. You can (and are encouraged to) use the calculational reasoning feature of Isar, but you can also use apply style or a mix of both to solve this question.

It is ok to look up the argument of the proof in a maths text book or on the web. The purpose of the question is to formalise the proof in Isabelle.