

COMP 4161 S2/08
Advanced Topics in Software Verification

Assignment 2

This assignment starts on Mon, 1.9.2008 and is due on Mon, 8.9.2008, 13:30h. Please submit electronically by email to gerwin.klein@nicta.com.au. Accepted formats are plain text, Isabelle theory files and pdf documents.

1 Proofs in Predicate Logic (39 marks)

Prove or disprove in Isabelle in single step proofs (rule/erule/drule/rule_tac, etc, but no blast or other automated methods).

- (a) $(\forall x. \forall y. R x y) = (\forall y. \forall x. R x y)$ (6 marks)
- (b) $((\exists x. P x) \vee (\exists x. Q x)) = (\exists x. (P x \vee Q x))$ (7 marks)
- (c) $((\forall x. P x) \wedge (\forall x. Q x)) = (\forall x. (P x \wedge Q x))$ (7 marks)
- (d) $\neg(\forall x. P x) \implies \exists x. \neg P x$ (6 marks)
- (e) $\neg(\exists x. P x) \implies \forall x. \neg P x$ (6 marks)
- (f) $(\forall x. P x \longrightarrow Q) = ((\exists x. P x) \longrightarrow Q)$ (7 marks)

2 Rich Grandmothers (21 marks)

Prove or disprove in Isabelle (in single step proof, no automated methods):

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

3 Proof Rules (10 marks)

Derive the classical contradiction rule $(\neg P \implies False) \implies P$ in Isabelle. Base your theory on theory Demo5 from lecture 8 instead of theory Main in HOL.

4 Automation (30 marks)

- (a) define `nor` and `nand` in Isabelle. (5 marks)
- (b) show `nor x x = nand x x` as a single step proof. (5 marks)
- (c) derive safe intro and elim rules for `nor` and `nand`. (15 marks)
- (d) use these in an automated proof of `nor x x = nand x x`. (5 marks)