Name: ....
Student Number ....

Software Engineering 2F04

DAY CLASS — Dr. Mark Lawford
DURATION OF EXAMINATION: 2 Hours
McMaster University Midterm Examination — November 1, 1999

THIS EXAMINATION PAPER INCLUDES 3 PAGES AND 4 QUESTIONS. YOU ARE RESPONSIBLE FOR ENSURING THAT YOUR COPY OF THE PAPER IS COMPLETE. BRING ANY DISCREPANCY TO THE ATTENTION OF YOUR INVIGILATOR.

Special Instructions: The use of calculators, notes, and text books is not permitted during this exam. Answer all questions in the provided answer booklets. Fill in your name and student number and sign each booklet you use.

1. Valid Rules of Inference (25 marks total)

In the course of answering this question you will hopefully convince yourself that the Rule of Indirect Proof (Rule IP) is a valid rule of inference.

a) A useful tautology

i) (2 marks) Write down the truth table for $P \to Q$.

ii) (3 marks) Use a truth table to verify that $\neg P \Leftrightarrow (P \to \bot)$

b) The Deduction Theorem

i) (5 marks) State the Deduction Theorem.

ii) (5 marks) Referring to your truth table in part (a)(i) above, explain intuitively why the deduction theorem is a valid rule of inference (i.e. why does it preserve truth).

c) (10 marks) Indirect Proof

Let Γ be a set of premises and P be an arbitrary propositional formula. Rule IP can be stated as follows:

$$\Gamma, \neg P \vdash \bot \text{ iff } \Gamma \vdash P$$

i) Show that if $\Gamma, \neg P \vdash \bot$ then $\Gamma \vdash P$. (Hint: Use parts (a) and (b) above.)

ii) Show that if $\Gamma \vdash P$ then $\Gamma, \neg P \vdash \bot$. (Hint: If Γ' is also a set of propositional premises such that $\Gamma \subseteq \Gamma'$ then for any formula Q if $\Gamma \vdash Q$ then $\Gamma' \vdash Q$.)

Congratulations! You've just shown that Rule IP is really just an application of Rule T with the tautology from (a) and the Deduction Theorem. (Not so mysterious after all, eh?)

2. Propositional Logic and Predicate Logic Basics (25 Marks)

a) (10 marks) Determine if the following set of premises is inconsistent:

$$\Gamma := \{A \to (B \leftrightarrow C), B \to D, B \vee C \to \neg D, A \wedge \neg D\}$$

Justify your answer.

Continued on page 2

b) (15 marks) Interpretation Structures and Validity of Arguments:
Find an interpretation structure $\mathbf{S} := \langle \mathbf{U}, \mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D} \rangle$ that demonstrates the following argument is invalid:
Premises: $(\forall x)(Ax \to Cx), (\forall x)(Bx \to Dx), (\exists x)Ax, (\exists x)\neg Dx$
Conclusion: $(\exists x)(Cx \land \neg Bx)$

3. More Propositional & Predicate Logic (25 Marks Total)

a) (10 marks) Verify that the following propositional formula is a tautology:

$$(P \to Q_1) \land (\neg P \to Q_2) \leftrightarrow (P \land Q_1) \lor (\neg P \land Q_2)$$

b) (10 marks) Prove that the following formula is a theorem of predicate logic:

$$(\forall x)(\forall y)[(Px \to Qyf(x)) \land (\neg Px \to Qyg(x))] \leftrightarrow (\forall x)(\forall y)[(Px \land Qyf(x)) \lor (\neg Px \land Qyg(x))]$$

c) (5 marks) The postcondition of the program statement

```
if (x>=3) y=x+1;
else y=1-x;
```

can be written as $(x \geq 3 \to y = x + 1) \land (x < 3 \to y = 1 - x)$. Find a logically equivalent formula ϕ that is a disjunction of two subformulas (i.e. ϕ is of the form $\phi_1 \lor \phi_2$).

4. Automated Verification of Propositional Logic (25 Marks Total)

Consider the set of premises:

$$\begin{aligned}\Gamma &:= \{P_1, P_2, \ldots, P_7\} \\ &= \{A \land C \to D, B \land C \to D, \neg(A \lor B) \to E \lor I, G \to \neg E, \neg I \lor H, C \land \neg D, G \to H\}\end{aligned}$$

i.e. P_1 will be a shorthand notation for $A \land C \to D$, P_2 will represent $B \land C \to D$, etc.

a) (5 marks)Applying the (BDDSIMP) command when trying to prove the PVS formula:

```
  a4:PROPOSITION (A AND C IMPLIES D) AND (B AND C IMPLIES D) AND
(NOT(A OR B) IMPLIES E OR I) AND (G IMPLIES NOT E) AND
(NOT I OR H) AND (C AND NOT D) AND (G IMPLIES H) => FALSE
```

results in several unprovable sequents. What do you conclude about the set of premises?

b) (5 marks) Two of the unprovable sequents resulting from applying the (BDDSIMP) command to the formula from (a) are shown below.

```
Sequent 1

{-1}    C
{-2}    E
  |-------
{1}    A
{2}    D
{3}    B
{4}    I
{5}    G
```

```
Sequent 2

{-1}    C
{-2}    I
{-3}    H
  |-------
{1}    A
{2}    D
{3}    B
{4}    E
```

Continued on page 3

i) Write down the characterisitic equation of each of the sequents.

ii) For each sequent, find a counter example that falsifies the sequent's characteristic equation.

iii) If you substituted either of these counter examples back into the premises of Γ, what would you find?

c) (10 marks) When the PVS prover is first started on the PROPOSITION above, it results in the sequent:

```
  |-------
{1}    (A AND C IMPLIES D)
          AND (B AND C IMPLIES D)
            AND (NOT (A OR B) IMPLIES E OR I)
              AND (G IMPLIES NOT E)
                AND (NOT I OR H) AND (C AND NOT D) AND (G IMPLIES H)
          => FALSE
```

If the command (FLATTEN) is applied to this sequent, it results in the sequent:

```
{-1}    (A AND C IMPLIES D)
{-2}    (B AND C IMPLIES D)
{-3}    (NOT (A OR B) IMPLIES E OR I)
{-4}    (G IMPLIES NOT E)
{-5}    (NOT I OR H)
{-6}    C
{-7}    (G IMPLIES H)
  |-------
{1}    D
```

Explain the proof steps that PVS performed to obtain this sequent.

d) (5 marks) For the set of premises Γ as defined above, it can be shown that $\Gamma \not\models C \wedge E$ and $\Gamma \not\models \neg(C \wedge E)$. Explain why this is possible. (HINT: See your answer to part (b) above!)

"What's the motivation for this section?" - 2F04 student

The End