UNIVERSITY OF WARWICK

Second Year Examinations: January 2009

Formal Specification and Verification

Time allowed: 2 hours.

Answer **FOUR** questions.

Read carefully the instructions on the answer book and make sure that the particulars required are entered on each answer booklet.

---

1. (a) Present the natural deduction rules:

   $\wedge$-elimination, $\rightarrow$-introduction, $\rightarrow$-elimination and $\vee$-elimination. [6]

   (b) Use the rules of natural deduction to prove the sequent:

   $p \rightarrow r \vee q \rightarrow r \vdash p \wedge q \rightarrow r$. [7]

   (c) By constructing a truth-table, or otherwise, determine whether the sequent:

   $$p \wedge q \rightarrow r \vdash p \rightarrow r \vee q \rightarrow r$$

   can be proved by natural deduction, stating any theorems you require. [7]

   (d) In the light of your answers, discuss whether the informal characterisation of implication, whereby $p \rightarrow q$ is interpreted as "q is true because p is true", is faithfully reflected in propositional logic. [5]

---

2. (a) Briefly explain what is meant by each of the following statements:

   i. the rules of natural deduction are *sound* for propositional logic;
   ii. the rules of natural deduction are *complete* for propositional logic;
   iii. provability by natural deduction is *decidable* for propositional logic;

   [6]

   (b) Describe the principles behind the proof of statement (ii) in (a) as clearly but concisely as you can, as if you were addressing your answer to a mathematician familiar with notions such as mathematical induction and the evaluation of boolean expressions. [16]

   (c) Which of the statements (i), (ii) and (iii) generalise to predicate logic? [3]

---

3. (a) What additional rules are introduced to generalise natural deduction from propositional to predicate logic? [5]

(b) Albert is trying to answer an examination question on logic: *"Prove that*

$$\neg(p_1 \wedge p_2) \vdash \neg p_1 \vee \neg p_2$$

using natural deduction, briefly explaining the proof rules required". He is trying to copy Victoria's answer, but unfortunately he can only see the left-hand side of her proof:

1.	$\neg(p_1 \wedge p_2)$	
2.	$\neg(\neg(p_1 \vee p_2))$	
3.	$\neg p_1$	assumption
4.	$\neg p_1 \vee \neg p_2$	$\vee i_1$ 3
5.	$\bot$	$\neg e$ 4,2
6.	p_1	PBC 3-5
7.	$p_1 \wedge p_2$	
8.	$\bot$	
9.	$\neg p_1 \vee \neg p_2$	

Provide Albert with a model answer. [7]

(c) Explain how your model answer in (b) can be generalised to a proof by natural deduction that

$$\neg\forall x P(x) \vdash \exists x \neg P(x)$$

[7]

(d) Discuss the most expressive ways of formalising the following statements using propositional and/or predicate logic:

i. If 18 is a prime number, then 2*4=6.
ii. The binary operator $\times$ is associative.
iii. There's an even number bigger than any given odd number, and vice versa.
iv. Albert has an ancestor called Victoria.

Give a brief justification for your answers. [6]

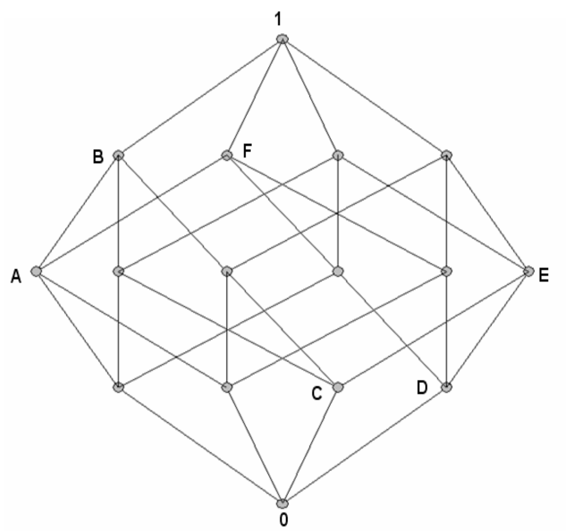
4. (a) A Boolean algebra has two binary operators $\wedge$ and $\vee$, a unary operator $\neg$, and two distinguished elements 0 and 1. What are the axioms to which these operators are subject? [4]

   (b) Prove that a Boolean algebra is partially ordered by the relation $\leq$ defined by

$$a \leq b \text{ if } a \wedge b = a.$$

[6]

   (c) Informally describe interpretations of the operators $\wedge$, $\vee$ and $\neg$, of the distinguished elements 0 and 1 that make the set of subsets of $\{1,2,3,4\}$ into a Boolean algebra. What is the partial order relation in this case? [4]



   (d) The above figure is a Hasse diagram H that represents the set of subsets of $\{1,2,3,4\}$. Given that the points A and B represent the subsets $\{3,4\}$ and $\{2,3,4\}$ respectively, determine what subsets are represented by the points C, D, E and F in H. [4]

   (e) The Hasse diagram H also represents a Boolean algebra defined by logically distinct propositions that can be expressed in terms of two atomic propositions p and q. What are the interpretations of the operators $\wedge$, $\vee$ and $\neg$ and of the distinguished elements 0 and 1 in this case? [3]

   (f) Suppose that A and B respectively represent the propositions p and p $\vee$ q. What propositions do the points C, D, E and F in H then represent? [4]

5. (a) What is meant by satisfaction of a Hoare triple $(\!|\phi|\!)\ P\ (\!|\psi|\!)$ under total correctness? [4]

   (b) What is meant by an *invariant* and a *variant* for a *while*-statement? [4]

   (c) What roles do invariants and variants play in establishing total correctness? [3]

   (d) Let `BinSize` denote the following code for computing the number of digits in the binary representation of a positive integer n:

```
y = 1;
z = 0;
while (y <= n) {
    y = 2*y;
    z = z+1;
}
```

   Show that `BinSize` meets its specification by constructing a proof tableau to establish that:

$$\vdash_{tot} (\!|n > 0|\!)\ \texttt{BinSize}\ (\!|y = 2^z \land y > n \land n \geq y/2|\!).$$

[14]