CS2420

UNIVERSITY OF WARWICK

Second Year Examinations: Sample paper

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) State the natural deduction rules: $\rightarrow$-introduction, $\rightarrow$-elimination, $\vee$-elimination, $\neg$-introduction, $\neg$-elimination. [8]

   (b) Prove $p \rightarrow (q \vee r), \neg q \vdash \neg r \rightarrow \neg p$ by natural deduction. [8]

   (c) Describe a procedure NNF(ϕ) which, given an implication-free propositional formula ϕ, returns a negation normal form for ϕ. [9]

---

2. (a) What does it mean for the set of rules of a deductive system to be *sound* and to be *complete*? [5]

   (b) Sketch a proof that the natural deduction rules are complete for propositional logic. [9]

   (c) Is natural deduction sound and complete for predicate logic? [3]

   (d) What does it mean to say that the algorithmic problem of determining the validity of a predicate logic formula is *undecidable*? [4]

   (e) What is the practical significance for automated reasoning of soundness, completeness and undecidability results in logic? [4]

---

3. (a) Write down a formula ϕ which is equivalent to $S(x) \wedge \forall y(P(x) \to Q(y))$, and such that $f(y, y)$ is free for x in ϕ. [8]

   (b) Explain what is meant by each of the following:

   i. a *model* of predicate logic;
   ii. an *environment* with respect to a model;
   iii. that $\phi_1, \cdots, \phi_n$ *semantically entail* ψ;
   iv. that $\phi_1, \cdots, \phi_n$ are *consistent*.

   [8]

   (c) Define $f^{\mathcal{M}}$ so that, together with the following definitions:

$$A = \{a, b, c, d\}$$

$$P^{\mathcal{M}} = \{(a, b), (b, c), (c, d), (d, a)\}$$

   we obtain a model $\mathcal{M}$ in which the formula $\neg\exists x P(f(x), x)$ is satisfied. [9]

---

4. (a) What is meant by satisfaction of a Hoare triple $(\!|\phi|\!)\ P\ (\!|\psi|\!)$ under partial correctness? What is meant by satisfaction of it under total correctness? [8]

   (b) State and briefly explain each of the following proof rules for partial correctness: `Composition`, `Assignment`, `If-statement`, `Partial-while`, `Implied`. [8]

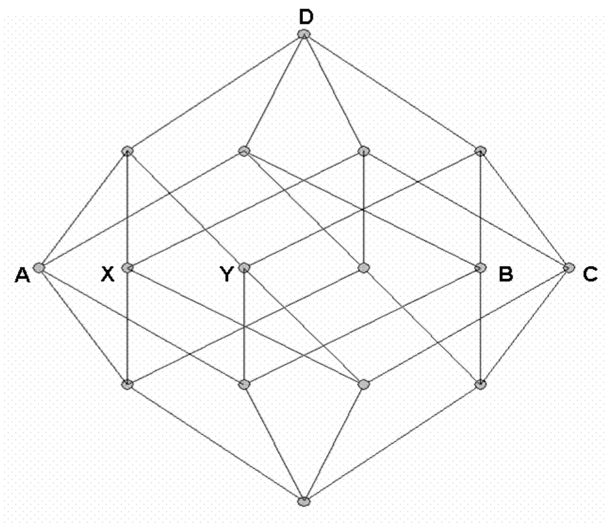
   (c) Let Div denote the following code:

```
z = 0;
while (x >= y) {
    z = z + 1;
    x = x - y;
}
```

   Show $\vdash_{tot} (\!|x = x_0 \wedge x \geq 0|\!)$ `Div` $(\!|x_0 = y \cdot z + x \wedge x < y \wedge x \geq 0|\!)$ by a proof tableau. [9]

5. (a) A *Boolean algebra* is a distributive lattice in which every element has a complement. Express this characterisation formally by explicitly stating the axioms that define a Boolean algebra. [5]

   (b) Prove that every element p in a Boolean algebra has a unique complement [5]



   (c) Suppose that the above figure is interpreted as a Hasse diagram representing the set of subsets of $\{1, 2, 3, 4\}$ ordered by inclusion, and that the points X and Y represent the subsets $\{1, 3\}$ and $\{2, 3\}$ respectively. Identify the subsets that are represented by the points A, B, C and D respectively. [5]

   (d) Suppose that the Hasse diagram is interpreted as representing the set of logically distinct propositional formulas that can be constructed from atomic propositions x and y ordered by the relation $\phi \leq \psi$ if and only if $\phi \to \psi$, and that x and y are represented by the points X and Y respectively. Identify four propositions that are represented by the points A, B, C and D respectively. [5]

   (e) Explain informally how you would use the Alloy tool to search for Boolean algebras with at most 8 elements. [5]