COMPUTER SCIENCE TRIPOS Part II

Tuesday 6 June 1995 1.30 to 4.30

Paper 7

Answer **five** *questions.*
Submit the answers in five **separate** *bundles each with its own cover sheet.*
Write on **one** *side of the paper only.*

1 Specification and Verification I

'A formally verified program is a correct program which will always work as required'.

Discuss the truth or otherwise of this statement with respect to

(a) capturing the specification [4 marks]

(b) the verification process [6 marks]

(c) using the program [8 marks]

In what circumstances might it be impossible formally to verify a program using a Hoare logic? [2 marks]

2 VLSI

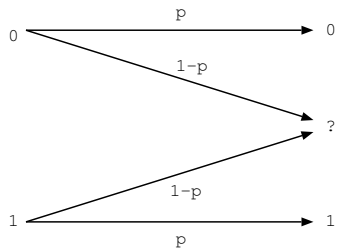
Give the transistor level design of a CMOS static 2-input NAND gate. [7 marks]

Sketch the layout of this gate either using stick diagrams or by showing the diffusion, polysilicon, and metal areas. [8 marks]

How could the characteristics of your design be altered to drive large loads in a symmetric way? [5 marks]

3 Information Theory and Coding

Give definitions and formulae for the mutual information and the capacity of a discrete memoryless channel. [8 marks]



The *binary erasure channel* (shown above) takes as input symbols '0' and '1' and outputs '0', '1', and '?' with the probability of correct reception of a symbol being p and of erasure $1 - p$. What is the capacity of this channel? [8 marks]

A particular serial line device acts as a binary erasure channel. It transmits characters as 8 bits, 7 bits of data and 1 parity check bit (obtained by an exclusive-or operation of the data bits); what is the probability that a received character cannot be decoded? [4 marks]

4 Distributed Systems

How does the requirement for replication and geographical distribution affect the handling of naming data in distributed systems? [10 marks]

Compare and contrast the requirements on databases used for naming data such as names to passwords and names to mailbox sites with the requirements on distributed financial data. [10 marks]

5 Philosophy

Discuss the logical status of *one* of the following: mental events, mathematical truths, ethical judgements. [20 marks]

6 Topics in Artificial Intelligence

Give some reasons why some tasks are suited to being solved by using *constraints*. Illustrate your answer with examples of such tasks and the methods by which constraints are used to solve them. [20 marks]

7 Computational Neuroscience

It has been said that there is no universal learning algorithm that can take a sample $S = \{\langle \mathbf{x}_i, f(\mathbf{x}_i)\rangle\}$ of training examples of an arbitrary unknown function f and produce a good approximation to f. Do you agree? Is such an algorithm possible? Discuss with reference to algorithms or methods and their assumptions and biases. [20 marks]

8 Security

Explain the difference between discretionary and mandatory access control. [3 marks]

Describe the Bell–LaPadula security policy model. [7 marks]

Discuss how one might implement a system enforcing the Bell–LaPadula model. [6 marks]

Explain what covert channels are, and how they can limit the usefulness of multilevel secure systems. [4 marks]

9 Pi Calculus

Define the term *sorting*, and explain what it means to say that a term of the π-calculus *respects* a given sorting. [5 marks]

Define the basic reduction rule COMM of the polyadic π-calculus. If $R \longrightarrow R'$ is an instance of COMM, and R respects a sorting ob, show that R' also respects ob. Argue informally that this holds for any reduction $R \longrightarrow R'$ whatever. [5 marks]

A labelled binary tree (lbt) is either a *node* with two sub-lbts, or else a *tip* with a label (some value). Show how to represent lbts uniformly as π-calculus agents with no free names. What sorting does your representation respect, given a sorting for label values? [7 marks]

Translate into the π-calculus the case-switch construction

$$\begin{aligned} &\mathit{case}\ t\ \mathit{of}\ \ ?\ \ \mathit{node}(t_1 t_2) \Rightarrow P \\ &\qquad\qquad\quad ?\ \ \mathit{tip}(v) \Rightarrow Q \end{aligned}$$

so that, when interacting with an lbt T located at t, it will enter P (with t_1, t_2 bound to the locations of the sub-lbts) if T is a node, and otherwise will enter Q (with v bound to the location of the label value). [3 marks]

10 Running a Business

The Wizzo project has two phases. Each phase consists of three main tasks: analysis, coding and test, which must be performed sequentially. Analysis for phase two can begin immediately on the completion of analysis for phase one, but coding for phase two must await satisfactory testing of the phase one code. Analysis is expected to take 3 weeks for phase one, and 4 weeks for phase two, while coding is expected to take 2 weeks for phase one and 3 weeks for phase two. Testing is expected to take 1 week for both phases.

(a) Draw the PERT and GANTT charts for the Wizzo project, and define the critical path. [5 marks]

(b) During testing of phase one a serious bug is found resulting in an extra 2 weeks' work required in that phase. How will this affect the overall timescale and critical path of the project? [5 marks]

(c) An extra programmer is assigned to the project in week 6, potentially increasing code productivity by 50%, but first requiring 1 week's training by the project analyst. Will this allow the project to finish early, with or without the event described in (b) above? [5 marks]

(d) What other tasks would you expect to be under the control of the Wizzo project manager and be included in a typical software project? [5 marks]

11 Specification and Verification II

Describe the choice operator, ε, of higher-order logic, giving examples of its use. [6 marks]

Using `First` and `Next`, where

```
First p t = (∀t'. t' < t ⇒ ¬(p t')) ∧ p t
Next p (t1,t2) = (t1 < t2) ∧ (∀t.t1 < t ∧ t < t2 ⇒ ¬(p t)) ∧ p t2
```

define a function `TimeOf` such that for a function, `f`, `TimeOf f n` returns the time when `f` becomes true for the $\mathtt{n}^{th}$ time. [4 marks]

Explain the significance of the following general theorem for temporal abstraction. Instantiate `r` and `f` for the case of a positive edge-triggered D-type flipflop, and describe what the general theorem states for these instantiations.

```
⊢ ∀f r.
    (∃t. f t) ∧
    (∀t. f t ⇒ (∃n. Next f (t,t+n) ∧ r(t,t+n))) ⇒
      (∀u. r(TimeOf f u,TimeOf f (u + 1)))
```

[10 marks]

12 Types

Give rules for deriving ML typing assertions of the form

$$x_1 : \sigma_1, \ldots, x_n : \sigma_n \vdash M : \sigma$$

You may assume that the types $\sigma_1, \ldots, \sigma_n, \sigma$ are built up from type variables and a type of booleans using function-, product-, and list-type constructors, and that the expressions M involve only identifiers, true, false, abstraction, application, projections, pairing, nil, cons, and let-declarations. [5 marks]

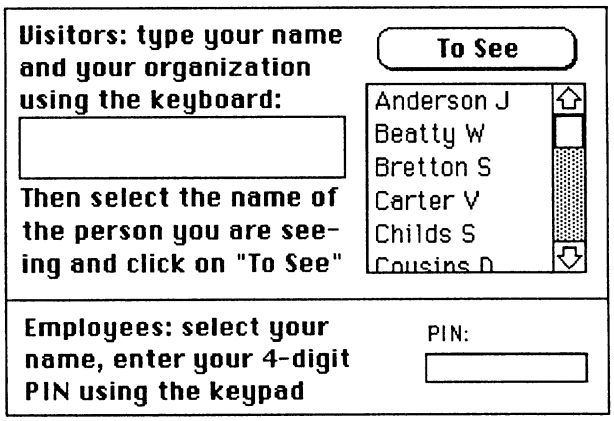
What does it mean for one ML type to be *more general* than another? What is meant by the *principal type* of a closed ML expression? [3 marks]

Give an account of an algorithm for deciding typability and producing principal types for the above fragment of ML. (Facts about unification may be quoted without proof.) [12 marks]

13 Designing Interactive Applications

At the reception desk of a highly secure organisation, all visitors and staff are required to register before entry to the building. The organisation's management is concerned to reduce registration delays without increasing levels of staffing at the desk.

(*a*) Write a one-sentence statement of a problem in interactive system design, aimed at addressing this situation. [3 marks]



(*b*) The figure above shows the screen layout of a possible system for visitor and staff registration, using multiple terminals, each equipped with display, keyboard, keypad and mouse. Name three methods you might use in assessing the usability of this design, and the reasons why each method might be useful. [5 marks]

(*c*) Describe, for the benefit of a new member of the design team, how to go about applying *one* of the three methods you have named in part (*b*). [8 marks]

(*d*) What interaction style, other than the direct-manipulation style illustrated in the figure, would be appropriate for this application,

14 Additional Topics

Discuss briefly the way in which a formal definition can assist the design and implementation of a programming language. [7 marks]

Explain the notion of a *delivery judgement* in Natural Semantics. Explain the ingredients of the judgement form

$$E \vdash_v exp \Rightarrow R$$

which represents the evaluation of an expression in Standard ML. Describe the rules which allow one to infer a judgement

$$E \vdash_v exp\ atexp \Rightarrow v$$

representing the application of a function to a value. [7 marks]

State the theorem which asserts the soundness of the Standard ML type discipline, explaining the notation used. How does this theorem help to reduce the number of evaluation rules which are necessary? [6 marks]

15 Additional Topics

What are the principal characteristics of an Active Badge? [8 marks]

Discuss three ways in which location information about personnel and equipment can be used in computer and communication systems. [12 marks]