COMPUTER SCIENCE TRIPOS Part II

Wednesday 1 June 1994 1.30 to 4.30

Paper 8

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 Additional Topics I and II

Cryptosystems can provide *confidentiality* or *integrity.* Consider two messages, one encrypted using a one-time pad and the other, a certificate signed using the private key from a public key system. Which of these two properties do each of these cryptosystems provide? [3 marks]

Explain why five-letter groups are sometimes used for encyphered messages. [4 marks]

Explain how a Vigenère cypher can be attacked. [9 marks]

Is this an asymmetric cypher? [2 marks]

Give a reason why an authentication service might be used instead of individuals sharing keys. [2 marks]

2 Distributed Systems

Explain how distributed inter-process communication (IPC) is supported in the following systems:

(*a*) BSD4.3 UNIX

(*b*) Mach

(*c*) ANSA

Your explanation should include naming and location as well as synchronisation and data transport. You should also mention any modes of IPC that are not supported. [20 marks]

3 Comparative Architectures

A naïve user translates the following C code:

```
extern int h(int *x, int flag);
int f(int *x) { return h(x, x[0]); }
int g(int *x) { return h(x + 2, (x[5]+x[6]) | 1); }
```

into the following assembly code for the MIPS R2000:

```
   .set    noreorder
   .globl  f,g       ; export f,g (implicitly import 'h')
f: lw      $5,0($4)  ; r4 holds 'x', load *x as 2nd argument
   j       h         ; tail-call to h
g: add     $4,$4,8   ; r4 holds 'x', load &x[2] as 1st argument
   lw      $5,12($4) ; r4 holds 'x+2', load x[5] as 2nd argument
   lw      $6,16($4) ; r4 holds 'x+2', load x[6] to a temporary
   add     $5,$5,$6  ; do the '+' ...
   or      $5,$5,1   ; ... and the '|'.
   j       h         ; tail-call to h
```

Each line of the above assembler program is individually a legal instruction or pseudo-instruction with valid comment. Explain in detail the effect of calling the assembler version of `f` with a suitable argument including a C function which exactly corresponds to the effect of the assembler version of `f`. [5 marks]

State the purpose of the `.set noreorder` directive. [2 marks]

Explain how the programmer has failed to understand the R2000 instructions and give a correct translation of the C code into assembly code (do not suggest removing the `.set noreorder` as part of the answer). [5 marks]

Explain briefly the origins of the errors (in both `f` and `g`) in terms of MIPS R2000 architecture. [5 marks]

How might knowing the first instruction of the compilation of `h()` affect your answer? [3 marks]

4 Digital Communication II

Describe the operation of private and public key encryption systems with an illustration of each. [12 marks]

End-to-end encryption is an OSI Presentation layer function; however, even when secure end-to-end encryption is employed, what forms of security attacks can be employed using information from the lower OSI layers? How can these be solved? [8 marks]

5 Information Theory and Coding

Define the Fourier Series of the periodic function $f(x)$ with period 2π, giving formulae for the Fourier Coefficients. [5 marks]

Derive the Fourier Coefficients for the Sawtooth function, the periodic function defined by

$$f(x) = x, -\pi < x < \pi$$

[10 marks]

The video drive circuitry of a computer monitor attempts to generate a periodic Sawtooth waveform to generate horizontal scanlines. However, the output circuitry is bandlimited to W; what would be the effect of this on the displayed pixels for various values of W? [5 marks]

6 Designing Interactive Applications

Pedal cyclists are to be allowed once again to ride through Cambridge on a 24-hour basis, using a traffic control system based on Air Traffic Control principles. By dialling a special telephone number and using the telephone keypad for data entry, cyclists will file a journey-plan before departure, and will be allocated a journey schedule that is announced back to them over the telephone.

Your company is bidding for the contract to develop the *journey-plan filing system*, which supports the filing of journey plans by the public and which will be linked to a separate system (not part of the bid) that controls cycle traffic. You have been put in charge of preparing your company's bid.

(*a*) Describe how you would conduct a user-needs analysis to support the design of the system. What are the main needs that you think would emerge from this? [6 marks]

(*b*) Design the user interface of the system in sufficient detail to explore the likely form of the user's mental model, and describe the form you think this mental model might take, presenting enough details of the user interface to justify your answer. [10 marks]

(*c*) How would you go about analysing and/or evaluating the design? [4 marks]

7 Optimising Compilers

Summarise *five* of the following ideas in *no more than* 150 words each:

(*a*) control flow determination in the presence of function or label variables

(*b*) safety of dataflow information

(*c*) basic blocks

(*d*) uses of live-variable information

(*e*) available expression analysis

(*f*) strictness

[4 marks each]

8 Artificial Intelligence I

Compare and contrast *heuristic search* and *exhaustive search.* [6 marks]

Which compromises are accepted by the heuristic approach? [8 marks]

Illustrate your answer with examples of heuristics. [6 marks]

9 Database Topics

Explain what is meant by saying that persistence of data is orthogonal to the syntax and semantics of the programming language PS-ALGOL. What criteria determine which data items will persist after a program has terminated? [8 marks]

In order to support database applications the PS-ALGOL run-time system handles transactions. Describe the relevant run-time system routines, and explain how serialisability is guaranteed. [6 marks]

How does the Persistent Object Management System ensure atomicity of database update? [6 marks]

10 Proving Programs Correct

Briefly discuss each of the following topics:

(*a*) partial and total correctness specifications [5 marks]

(*b*) goal-directed proof using verification conditions [5 marks]

(*c*) reasoning about arrays [5 marks]

(*d*) use of Floyd–Hoare logic to provide an *axiomatic semantics* for programming languages [5 marks]

11 Specification and Verification of Hardware

Briefly discuss each of the following topics:

(*a*) the representation of schematic diagrams in predicate calculus [5 marks]

(*b*) the use of primitive recursion in hardware specification [5 marks]

(*c*) modelling combinational and sequential circuits [5 marks]

(*d*) temporal abstraction [5 marks]

12 Semantics of Programming Languages

Let D be a complete partial order with bottom. What does it mean for a subset of D (regarded as a predicate) to be *inclusive*? State Scott's principle of fixed-point induction. [6 marks]

Let $\mathbf{B}$ be the usual flat complete partial order of truth values consisting of elements $\perp$, $true$ and $false$. For a complete partial order D with bottom, let the conditional function

$$\cdot \to \cdot \,|\, \cdot \quad : \quad \mathbf{B} \times D \times D \longrightarrow D$$

be given by

$$b \to d \,|\, e \quad = \quad \begin{cases} d & \text{if } b = true, \\ e & \text{if } b = false, \\ \perp & \text{if } b = \perp. \end{cases}$$

Let $p : D \longrightarrow \mathbf{B}$ and $h : D \longrightarrow D$ be continuous functions with h strict (i.e. $h(\perp) = \perp$). Let $f : D \times D \longrightarrow D$ be the least continuous function which satisfies

$$f(x,y) \quad = \quad p(x) \to y \,|\, h(f(h(x),y)) \qquad \text{for all } (x,y) \in D \times D.$$

Show that the following predicate

$$P(g) \quad \equiv \quad \forall (x,y) \in D \times D . h(g(x,y)) = g(x,h(y))$$

is inclusive. [4 marks]

Prove that $h(f(x,y)) = f(x,h(y))$, for all $(x,y) \in D \times D$. [10 marks]

13 Types

Explain what is meant by saying that a programming language is

(a) strongly typed

(b) monomorphic

(c) polymorphic

[4 marks]

Briefly describe some ways in which polymorphism may arise in programming languages. [5 marks]

Consider extending the ML type inference system with a new type constant ω and a type inference rule

$$\text{(UNIV)}\,\frac{}{\Gamma \vdash M : \omega}$$

where M is any expression and Γ is any context assigning types to a finite set of identifiers that includes the free identifiers in M. Prove that

$$\vdash FF : (\omega \to \sigma) \to \sigma$$

holds in this extended system, where σ is any type and F is the expression

$$\lambda y.\lambda x.x((yy)x)$$ [6 marks]

Do closed expressions possess *principal* types in this extension of ML?
[Hint: consider the possible types $\lambda x.x$ may possess in this system.] [5 marks]

14 Concurrency

What is meant by a *strong bisimulation* on CCS agents? How are strong bisimulations used to show that two agents are strongly equivalent? [5 marks]

Suppose that $M = (Q, \Sigma, \Delta, i, F)$ is a finite non-deterministic automaton with set of states Q, input alphabet Σ, transition relation $\Delta \subseteq Q \times \Sigma \times Q$, initial state i, and set of accepting states F. Show how to define CCS agents A_q (for each state $q \in Q$) and *Stop* with the properties

$$\begin{aligned} A_{q_1} \xrightarrow{a} A_{q_2} &\quad \text{if and only if} \quad (q_1, a, q_2) \in \Delta \\ A_q \xrightarrow{\tau} B &\quad \text{if and only if} \quad B = \mathit{Stop} \text{ and } q \in F \end{aligned}$$

for all $q_1, q_2, q \in Q$, all $a \in \Sigma$, and all agents B. [5 marks]

Suppose that $M' = (Q', \Sigma, \Delta', i', F')$ is another finite non-deterministic automaton (over the same input alphabet) and corresponding CCS agents $A'_{q'}$ ($q' \in Q'$) and Stop' are defined for M' as above. Show that the languages accepted by M and M' are equal if A_i and $A_{i'}$ are strongly equivalent CCS agents. [6 marks]

Is the converse true? [4 marks]