COMPUTER SCIENCE TRIPOS Part II

Tuesday 2 June 1998 1.30 to 4.30

Paper 7

Answer **five** *questions.*
Submit the answers in five **separate** *bundles, each with its own cover sheet. On each cover sheet, write the numbers of* **all** *attempted questions, and circle the number of the question attached.*
Write on **one** *side of the paper only.*

1 VLSI

Give the circuit for a CMOS inverter. [4 marks]

Give layouts for CMOS inverters of the following types:

(a) basic design using one layer of metal

(b) basic design using two layers of metal

(c) an advanced design for driving large loads

[4 marks each]

What is the purpose of a buffer chain when distributing the clock? [4 marks]

2 Specification and Verification I

Describe briefly the difference between *soundness* and *completeness* for a logic. [4 marks]

Consider the following possible assignment axioms:

(*a*) $\{P\}\ V\ \texttt{:=}\ E\ \{P[E/V]\}$

(*b*) $\{P[E/V]\}\ V\ \texttt{:=}\ E\ \{P\}$

(*c*) $\{P\}\ V\ \texttt{:=}\ E\ \{P\ \wedge\ V = E\}$

(*d*) $\{P\ \wedge\ V = E\}\ V\ \texttt{:=}\ E\ \{P\}$

For each of these *either* give a brief informal argument why it is sound, *or* give a counterexample. [8 marks]

If V is a variable, let $V\texttt{++}$ be a C-like expression that returns the value of V and then increments it. Describe why the simple Hoare assignment axiom is not valid if such expressions are allowed. [2 marks]

Consider a C-like operator `+=` whose semantics is that $V\ \texttt{+=}\ E$ adds the value of E to V. Write down an axiom for such an assignment and informally justify its soundness. [2 marks]

Write down a sound axiom for a parallel assignment

$$V_1, \ldots, V_n\ \texttt{:=}\ E_1, \ldots, E_n$$

($E_1, \ldots, E_n$ are simultaneously assigned to $V_1, \ldots, V_n$). [2 marks]

Is this equivalent to the sequence of single assignments

$$V_1\ \texttt{:=}\ E_1\texttt{;}\ \ldots\ \texttt{;}V_n\ \texttt{:=}\ E_n?$$

Justify your answer. [2 marks]

3 Comparative Architectures

Older computer architectures often contain features that hamper high-performance implementation using modern techniques. Describe several such features, explaining how they affect implementation; describe what techniques (if any) have been developed to help overcome these difficulties. [14 marks]

The original MIPS architecture (as implemented in the R2000) relied on software interlocking of pipeline stages, thus exposing load and branch delays to the compiler which is then responsible for scheduling instructions to avoid conflicts.

Assess the pros and cons of software interlocking at the time of the introduction of the R2000. How has the situation changed for modern high-performance MIPS implementations? [6 marks]

4 ECAD Topics

Explain the purpose and principles of fault simulation in electronic CAD. Why is it difficult to implement efficiently? [4 marks]

Describe the following three techniques for fault simulation:

(a) parallel fault simulation [4 marks]

(b) concurrent fault simulation [4 marks]

(c) deductive fault simulation [4 marks]

Which of these schemes would be suitable for higher-level functional units rather than gates? In particular, how would they handle logic blocks with internal state? [4 marks]

5 Denotational Semantics

Suppose that D is a domain and that $lam : (D \to D) \to D$ and $app : D \to (D \to D)$ are continuous functions. Using D, lam and app, you are required to give a denotational semantics to the terms of the untyped lambda calculus: $M ::= x \mid \lambda\, x\, (M) \mid M\, M$, where x ranges over some fixed, infinite set of variables and where terms are identified up to alpha-conversion. For each term M and list $\vec{x} = x_1, \ldots, x_n$ of distinct variables containing the free variables of M, define a continuous function

$$\rho \mapsto [\![\vec{x} \vdash M]\!](\rho)$$

mapping elements ρ of the product domain D^n (regarded as functions from $\{x_1, \ldots, x_n\}$ to D) to elements of D. The definition should proceed by induction on the structure of M and you should state clearly, but without proof, any properties of continuous functions between domains which are needed for the definition to make sense. [10 marks]

Show, by induction on the structure of M, that the following substitution property holds:

$$[\![\vec{x} \vdash M[M'/x]]\!](\rho) = [\![\vec{x}, x \vdash M]\!](\rho[x \mapsto [\![\vec{x} \vdash M']\!](\rho)]).$$

(You may assume without proof that $[\![\vec{x}, x \vdash M]\!](\rho[x \mapsto d]) = [\![\vec{x} \vdash M]\!](\rho)$ when x does not occur free in M.) [5 marks]

Show that if the composition $app \circ lam$ is the identity function on the function domain $D \to D$, then the denotational semantics respects beta-reduction, in the sense that $[\![\vec{x} \vdash (\lambda\, x\, (M))\, M']\!](\rho) = [\![\vec{x} \vdash M[M'/x]]\!](\rho)$. [3 marks]

What condition on lam and app will ensure that eta-reduction, $\lambda\, x\, (M\, x) \to M$ (where x is not free in M), is respected? [2 marks]

6 Artificial Intelligence

Describe, with examples, *four* problems that might be encountered when attempting to use automatic planning techniques. [5 marks per problem]

7 Neural Computing

In Computer Science, a fundamental distinction has classically been erected between computing and communications. The former creates, requires, or manipulates data, and the latter moves it around. But in living neural systems, this distinction is less easy to establish; a given neurone performs both functions by generating nerve impulses, and it is not clear where to draw the distinction between processing and communication. The problem is even more obvious in artificial neural networks, where the entire essence of computing is modelled solely as changes in connectivity. Flesh out and discuss this issue. Would you argue that some of the limitations of efforts in artificial intelligence have been the result of such a spurious dichotomy?

[20 marks]

8 Database Topics

Describe the main features of the Data Language DAPLEX, paying particular attention to the following points:

(a) schema definition and maintenance

(b) primitive and derived data

(c) entity specialisation

(d) consistency constraints

[9 marks]

Explain how aggregates are handled in DAPLEX, paying particular attention to the following:

(e) composition of many-valued functions

(f) calculation of averages

(g) inverse functions

(h) multiple inheritance

[7 marks]

The DAPLEX paper received a great deal of attention when it appeared in 1981. Why do you think that was, and why is the work largely forgotten today?

[4 marks]

9 Security

Describe the purpose of hash functions, message authentication codes and digital signatures, sketching a possible construction for each of them. [12 marks]

A funds transfer system authenticates messages between its member banks by having the sending and receiving banks compute a MAC on each message using a key which each pair of correspondent banks in the system establishes monthly using public key techniques. The sending bank then computes a digital signature on the MAC using a long-term signing key.

If the MAC is 32 bits long, is this arrangement more, or less, secure than signing a 128-bit hash of the message, and why? [5 marks]

To what extent would matters be changed if all messages handled by the system were logged by a trusted third party? [3 marks]

10 Types

Each natural number $n \in \mathbb{N}$ can be encoded in the polymorphic lambda calculus (PLC) by the beta-normal form $Num_n \stackrel{\text{def}}{=} \Lambda\,\alpha\,(\lambda\,x : \alpha\,(\lambda\,f : \alpha \to \alpha\,(f^n x)))$, where the expression $f^n x$ is an abbreviation for the PLC expression inductively defined by

$$f^0 x \stackrel{\text{def}}{=} x \qquad \text{and} \qquad f^{n+1} x \stackrel{\text{def}}{=} f\,(f^n x).$$

For which PLC type nat does $\vdash Num_n : nat$ hold? [3 marks]

Say that a function $\phi : \mathbb{N} \to \mathbb{N}$ is *PLC-representable* if there is a PLC expression F such that the following typing and beta-conversions hold:

$$\vdash F : nat \to nat \qquad \text{and} \qquad F\,Num_n =_\beta Num_{\phi(n)} \quad (\text{all } n \in \mathbb{N}).$$

Show that the successor function, $s(n) \stackrel{\text{def}}{=} n + 1$, is PLC-representable. [5 marks]

Given a PLC-representable function ϕ and a number $a \in \mathbb{N}$, show that the function ψ inductively defined by

$$\psi(0) \stackrel{\text{def}}{=} a \qquad \text{and} \qquad \psi(n+1) \stackrel{\text{def}}{=} \phi(\psi(n))$$

is PLC-representable. [8 marks]

Is every function $\mathbb{N} \to \mathbb{N}$ PLC-representable? Justify your answer. [4 marks]

11 Specification and Verification II

Describe informally the meaning of the following four CTL operators: AX, EX, $A[\cdots U \cdots]$, $E[\cdots U \cdots]$. [4 marks]

Describe how CTL operators can be defined in higher order logic. [4 marks]

Hence or otherwise show that $A[true\ U\ P]$ holds if P holds somewhere along every path. [2 marks]

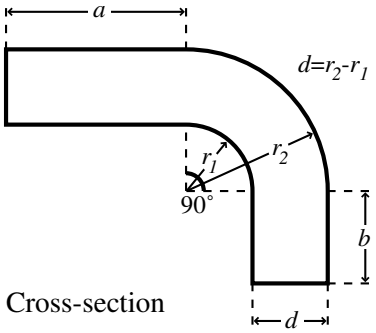
Define $AG\ P \equiv \neg E[true\ U \neg P]$ and show that $AG\ P$ holds if P holds everywhere along every path. [4 marks]

Express "if P is ever true, then it continues to be true until Q is false" in CTL. [3 marks]

Describe in English the meaning of $AG(P \wedge Q \Rightarrow AX(A[P\ U\ \neg Q]))$. [3 marks]

12 Advanced Graphics

Perspective view

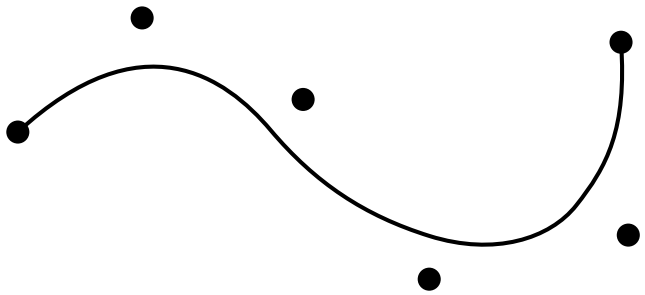


Show how the above object can be constructed using Constructive Solid Geometry (CSG). You may assume the following primitives: sphere, cylinder, cone, torus, box. [4 marks]

Show how the same object can be constructed as a swept object. [3 marks]

Explain how you would convert the swept object into polygons. [4 marks]

What extra work would you need to do if you had to convert it into triangles? [1 mark]



Consider the design of a user interface for a NURBS drawing system, which enables curves like that above to be drawn. Users should have access to the full expressive power of the NURBS representation. What things should users be able to modify to give them such access and what effect does each have on the resulting shape? [6 marks]

Users will need to select the control points for curves like that drawn above. You need to decide the size to draw the control points. What does Fitts' Law tell you about how choice of size affects user interaction speed? [2 marks]

13 Natural Language Processing

Write about *three* of the following problems, describing the issues they raise for natural language processing and possible techniques for dealing with them.

(a) The morphological decomposition and semantic interpretation of the following words:

reuse versus *react*
thinker versus *washer* versus *beggar*
decentralisation

(b) The syntactic ambiguity introduced by rules such as N $\rightarrow$ N N for noun compounds.

(c) The resolution of the potential ambiguity in *List the Frenchman among the programmers who understand*(s) *English* through the use of agreement features.

(d) The representation and recovery of the semantic interpretation of *Every company gave its representative a car* and the resolution of quantifier scope ambiguity.

(e) The representation and recovery of the anaphoric and referential links in the following discourse:

John saw a house he liked. The windows were large and the door was varnished. He wanted to go inside it.

[20 marks]

14 Additional Topics

What is the Active Badge? [5 marks]

Describe *five* different applications which are made possible by information supplied by the Active Badge. [10 marks]

"Many future applications will take advantage of location information." Discuss. [5 marks]

15 Additional Topics

Explain the ingredients of the judgement form

$$E \vdash_v exp \Rightarrow R$$

which represents the evaluation of an expression in Standard ML. Explain also how, in a fuller form, it caters for side-effects in expression evaluation, and illustrate this using one of the evaluation rules. [7 marks]

State two theorems about evaluation in Standard ML: one which asserts that it is deterministic, and another which asserts that pattern-matching has no side-effects. [6 marks]

Explain how the raising and handling of exceptions is expressed in the evaluation rules. [7 marks]