COMPUTER SCIENCE TRIPOS Part Ib

Monday 6 June 2005 1.30 to 4.30

Paper 3

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.*

You may not start to read the questions printed on the subsequent pages of this question paper until instructed that you may do so by the Invigilator

STATIONERY REQUIREMENTS
Script Paper
Blue Coversheets
Tags

1 ECAD

(a) What input condition will cause a D flip-flop to go metastable? [3 marks]

(b) What timing parameters have to be adhered to in order to avoid metastability? [3 marks]

(c) Will a D flip-flop remain in the metastable state indefinitely? [3 marks]

(d) What is the difference between synchronisation and debouncing? [3 marks]

(e) How is a synchroniser made out of D flip-flops? [3 marks]

(f) What are the failure modes for the following two counters (`count0` and `count1`) if `asyncInput` comes from a synchronous digital circuit clocked from a different clock source and `keyInput` comes directly from a mechanical push button?

```
reg [63:0] count0, count1;
reg [2:0]  sync;
always @(posedge clock)
  begin
    // count how many clock cycles asyncInput is high
    if(asyncInput) count0 <= count0+1;
    // count the number of times the keyInput is pressed
    sync <= {sync[1:0],keyInput};
    if(!sync[2] && sync[1]) count1 <= count1+1;
  end
```

[5 marks]

2 Data Structures and Algorithms

(*a*) Briefly outline how a sequence of symbols can be encoded as a sequence of Huffman codes, and explain under what assumptions Huffman encoding generates optimally compact code. [6 marks]

(*b*) Estimate the number of bits needed to Huffman encode a random permutation of `A`s, `B`s and `C`s, with each letter occurring one million times. [3 marks]

(*c*) Estimate the number of bits needed to Huffman encode a random permutation of `A`s, `B`s and `C`s, where `A` occurs two million times and `B` and `C` each occur one million times. [3 marks]

(*d*) Estimate how many bits would be needed to encode the sequence in part (*b*) above using arithmetic coding. You may assume that $\log_2 3$ is about 1.6. [4 marks]

(*e*) Estimate, with justification, how many bits would be needed to encode the sequence in part (*c*) above using arithmetic coding. [4 marks]

3 Artificial Intelligence I

(*a*) What are the advantages and disadvantages of *constraint satisfaction problem* (CSP) solvers compared with search algorithms such as $A^\star$ search, etc? [3 marks]

(*b*) Give a general definition of a CSP. Define the way in which a solution is represented and what it means for a solution to be *consistent* and *complete*. [5 marks]

(*c*) Assuming discrete binary constraints and finite domains, explain how breadth-first-search might be used to find a solution and why this is an undesirable approach. [3 marks]

(*d*) Give a brief description of the basic *backtracking algorithm* for finding a solution. [4 marks]

(*e*) Describe the *minimum remaining values heuristic*, the *degree heuristic* and the *least constraining value heuristic*. [5 marks]

4 Comparative Programming Languages

Consider the Prolog procedures named `s` and `p` defined as follows:

```
s(H, [H|T], T).
s(H, [N|T], [N|L]) :- s(H, T, L).

p(X, [H|T]) :- s(H, X, Z), p(Z, T).
p([], []).
```

(*a*) Show how Prolog would evaluate the goal `s(H, [a,b,c], T)` giving all the successive instantiations of `H` and `T` that cause the goal to be satisfied, and hence describe in words what `s` does. [6 marks]

(*b*) What value of `Q` causes the goal `p([a], Q)` to be satisfied? [3 marks]

(*c*) What values of `Q` cause the goal `p([a,b], Q)` to be satisfied? [4 marks]

(*d*) What values of `Q` cause the goal `p([a,b,c], Q)` to be satisfied? [5 marks]

(*e*) Describe in words what `p` does. [2 marks]

5 Operating Systems II

(*a*) Modern operating systems typically support both *threads* and *processes*. What is the basic difference between a thread and a process? Why do operating systems support both concepts? [2 marks]

(*b*) You get a summer job with a company which has an in-house operating system called sOs. sOs uses static priority scheduling, supports at most 32 concurrently-executing processes, and works only on uniprocessor machines. Describe with justification how you would modify sOs in order to:

(*i*) support up to 50000 concurrently executing processes; [2 marks]

(*ii*) reduce or eliminate the possibility of starvation; [3 marks]

(*iii*) efficiently schedule processes on an 8 CPU symmetric multiprocessor (SMP) machine; [5 marks]

(*iv*) support threads in addition to processes on SMP machines. [3 marks]

(*c*) How would you go about reducing the time taken to boot a modern operating system? [5 marks]

6 Numerical Analysis I

(*a*) The parameters for *IEEE* Single Precision are: $\beta = 2$, $p = 24$, $e_{min} = -126$, $e_{max} = 127$. Explain the terms *significand*, *sign bit*, *exponent*, *normalised number*, *denormal number*, *hidden bit*, *precision* as used in *IEEE* Single Precision. [7 marks]

(*b*) Let ω represent any of the operations $+ \ - \ * \ /$. Let x be a positive finite representable number. List what each of the following evaluates to for each operation:

$$(+\infty)\ \omega\ x$$
$$x\ \omega\ (-\infty)$$

[Show the sign of your answer in each case.] [4 marks]

(*c*) Suppose the principles of *IEEE* arithmetic are applied to a floating-point representation with 6 bytes (48 stored bits). If $\beta = 2$, $e_{max} = 511$ and a hidden bit is used, deduce the values of e_{min} and p. [4 marks]

(*d*) Define *machine epsilon* ε_m. [1 mark]

(*e*) The function

$$f(x) = \frac{(x+1)^2}{x^2+1}$$

is to be evaluated using *IEEE* arithmetic for $x \geq 0$. Re-write the formula so that $f(x)$ can be evaluated in the case where x is representable but x^2 overflows. What does your formula evaluate to in the case that $(1/x) < \varepsilon_m$? [4 marks]

7 Computation Theory

(*a*) Explain informally, i.e. without reference to any particular model of computation, why the *Halting Problem* is undecidable. [6 marks]

(*b*) Briefly describe two mathematical problems, other than the Halting Problem, that are algorithmically undecidable. [4 marks]

(*c*) What does it mean for a partial function to be *register machine computable*? Show how the informal argument in part (*a*) can be turned into a rigorous proof that there is no register machine deciding the Halting Problem for register machine computable functions. [10 marks]

8 Computer Graphics and Image Processing

(*a*) Calculate the maximum resolution needed by a movie projector in a movie theatre. Clearly state any assumptions that you make. [6 marks]

(*b*) Describe, in detail, an error diffusion algorithm for converting greyscale images to bi-level black and white images at the same resolution. [8 marks]

(*c*) Explain how this could be extended to provide an algorithm to print full colour RGB images on a CMYK laser printer, assuming that one pixel in the image maps to one pixel on the printer. [6 marks]

9 Introduction to Security

(*a*) A and B play a simple game. A chooses a number $R_A \in \mathbb{Z}_3$ and B chooses a number $R_B \in \mathbb{Z}_3$. Then A and B communicate their respective choice to each other *simultaneously*, meaning that the players cannot change their choice after having seen that of the opponent. These rules decide who wins the game:

$$\begin{aligned} R_A &\equiv R_B + 1 \pmod 3 \quad \Rightarrow \quad A \text{ wins} \\ R_B &\equiv R_A + 1 \pmod 3 \quad \Rightarrow \quad B \text{ wins} \end{aligned}$$

In any other case, the result of the game is a draw.

(*i*) What complication arises when this game is played at a distance, for example via e-mail? [2 marks]

(*ii*) Suggest a cryptographic protocol that prevents cheating when this game is played via e-mail. Your solution should not rely on a trusted third party. [6 marks]

(*iii*) What assumptions do you make about the cryptographic functions used in your solution of part (*ii*)? [3 marks]

(*iv*) What assumptions do you make about the amount of computing power available to the opponent in your solution of part (*ii*)? [3 marks]

(*b*) Outline briefly the purpose of an organisation's security policy and what steps should be considered in its development. [6 marks]

END OF PAPER