

## COMPUTER SCIENCE TRIPOS Part IA

---

Tuesday 4 June 2019 1.30 to 4.30

---

### COMPUTER SCIENCE Paper 2

Answer **one** question from each of Sections A, B and C, and **two** questions from Section D.

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 cover sheets*

*Tags*

#### SPECIAL REQUIREMENTS

*Approved calculator permitted*

## SECTION A

## 1 Digital Electronics

(a) (i) Show that

$$A + B.C = (A + B).(A + C) \quad [2 \text{ marks}]$$

(ii) Using the distributive law in Part (a)(i), express the following equation in product of sums form with 4 product terms, each with a sum of 3 variables:

$$F = H + I.\bar{J} + \bar{K}.L \quad [4 \text{ marks}]$$

(b) (i) Write down the truth table for the logic unit (LU) defined in the following table that can execute one of 4 logical operations at a time on 2 data inputs ( $Y_1, Y_0$ ), to yield output ( $Z$ ). The LU is under the control of inputs ( $I_1, I_0$ ) and the logical operations are encoded to 2-bit instruction codes as follows:

Operation	OR	AND	XOR	NOP
Instruction code ( $I_1 I_0$ )	00	01	10	11

Note that operations OR, AND and XOR have their usual meanings and that the execution of NOP implies  $Z$  can take any binary value.

[3 marks]

(ii) Use a Karnaugh Map to determine a simplified expression for  $Z$  in Part (b)(i). [2 marks]

(c) (i) Show using a circuit diagram how  $W$  can be implemented in 2-level sum of products form using AND gates followed by OR gates. Remember to include any NOT gates required since only uncomplemented input variables are available:

$$W = \bar{B}.\bar{C} + \bar{A}.B.C + A.C.\bar{D}$$

[2 marks]

(ii) Consider the implementation in Part (c)(i). Assume that the gates have finite propagation delay. Describe what happens at  $W$  when inputs  $\{A, B, C, D\}$  change from  $\{1, 0, 1, 0\}$  to  $\{1, 0, 0, 0\}$ .

[3 marks]

(iii) Determine the other single input variable change that will give a similar problem to that observed in Part (c)(ii).

[2 marks]

- (iv) Determine a modified sum of products expression for  $W$  that will eliminate the problems observed in Part (c)(ii) and Part (c)(iii).

[2 marks]

## 2 Digital Electronics

- (a) (i) Briefly describe the ways in which sequential logic differs from combinational logic.

[2 marks]

- (ii) Describe the main features that differentiate synchronous from asynchronous sequential logic.

[4 marks]

- (b) A synchronous 3-bit counter implemented using D-type Flip-Flops has a mode control input  $M$ . When  $M = 0$ , the counter output sequence represented in decimal form is 0, 1, 2, 3, 4, 5, 6, 7, and repeat. When  $M = 1$ , the counter output sequence represented in decimal form is 0, 1, 3, 2, 6, 7, 5, 4, and repeat. The Flip-Flop outputs are  $\{Z_2Z_1Z_0\}$  where  $Z_0$  represents the least significant bit of the counter output.

- (i) Draw a state diagram that describes this counter.

[4 marks]

- (ii) Write down the state transition table corresponding with the state diagram in Part (b)(i).

[2 marks]

- (iii) Determine the excitation combinational logic in sum of products form for D-type Flip-Flop input  $D_0$ , i.e., the input of the Flip-Flop that represents the least significant bit of the counter. Show that the required combinational logic can be implemented using a 2-input XNOR gate plus some other combinational logic gates.

[3 marks]

- (c) Use row matching to reduce the number of states required to represent the single input ( $X$ ), single output ( $Z$ ), Mealy finite state machine described in the following state transition table:

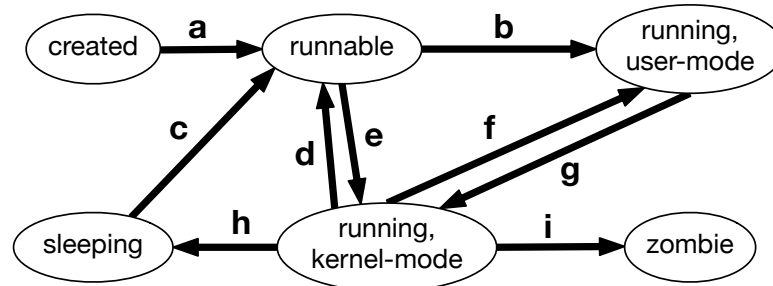
Current State	Next State		Output ( $Z$ )	
	$X = 0$	$X = 1$	$X = 0$	$X = 1$
A	B	C	1	0
B	F	D	0	0
C	D	E	1	1
D	F	E	0	1
E	A	D	0	0
F	B	C	1	0

Draw the resulting state diagram.

[5 marks]

## SECTION B

## 3 Operating Systems



- (a) The diagram above is a simplified state machine for processes in a UNIX operating system. For each of the following, give the state transition(s) taken by the process, and state whether or not the scheduler runs.
- (i) A running user process is interrupted by a timer, whose interrupt handler determines it has used all of its allocated time slice. [2 marks]
- (ii) A running user process invokes a non-blocking asynchronous IO operation. [2 marks]
- (iii) A single-threaded running user process invokes a blocking synchronous IO operation that takes some considerable time to return. [2 marks]
- (b) Assume the process scheduler is *pre-emptive*. Which transitions will cause it to be entered? If it were replaced with a *non-preemptive* scheduler, which transitions would now cause the process scheduler to be entered? [6 marks]
- (c) Consider three CPU-bound processes arriving to a First Come First Served (FCFS) scheduler as follows:

Process	Arrival Time	Duration
P <sub>1</sub>	0	3
P <sub>2</sub>	1	12
P <sub>3</sub>	5	1

Give the schedule computed, and the average waiting time across all three processes. [3 marks]

- (d) A weakness of FCFS is that its performance is sensitive to the arrival process. Assume process arrival times remain  $t = 0, 1, 5$  but the arrival order changes. Give an alternative arrival order that improves the average waiting time. Define the *convoy effect* and give a second alternative arrival order displaying it. [5 marks]

## 4 Operating Systems

- (a) Describe the mechanisms by which an operating system protects a user process' use of system resources (CPU, memory, IO) from accidental or deliberate interference by other processes. Indicate what special hardware, if any, is required for each mechanism. [6 marks]
- (b) Inter-Process Communication (IPC) requires that two processes on the same host can somehow share information directly. Why does this require special support in the operating system? Compare the following IPC mechanisms in terms of how easily they support interaction between processes: *UNIX signals, pipes, named pipes*. [6 marks]
- (c) In UNIX, files are usually protected using *access control lists*, with the access control check carried out when the file is opened. What would be the trade-off if the access control check were instead performed when the file was written or read? Describe how you might implement a capability system to protect files from access, give a possible API, and compare your proposal to the UNIX access control method. [8 marks]

## SECTION C

### 5 Software and Security Engineering

PenAMessage is a text messaging platform written by a start-up. A potential buyer is considering hiring you to conduct an audit.

- (a) The potential buyer interviews you to assess your background. For each pair of terms, discuss whether the terms are equivalent.
- (i) error and failure
  - (ii) hazard and risk
  - (iii) safety and reliability
  - (iv) dependability and security

[8 marks]

The potential buyer decides to hire you. The CTO of the start-up explains that users register by installing the PenAMessage app on their smartphone. On registration, the app sends the phone number of the smartphone together with a list of all phone numbers found in the contact address book to a single physical server operated by PenAMessage. The server responds with a list of those contacts in the address book who are registered users. Registered users send messages to one another using the app; all such messages are sent via the server.

- (b) Write down four major elements of the PenAMessage system which you will consider as part of your audit. [4 marks]
- (c) Describe how the failure of each element you selected in Part (b) might affect overall system dependability, user privacy and security. State any assumptions you make about the architecture and implementation of PenAMessage. [4 marks]
- (d) Describe the approach you would take to identify the most important risks to the security of PenAMessage. [4 marks]



## 6 Software and Security Engineering

EvaCam is an Internet-enabled camera platform intended for use by consumers to continuously monitor their homes for suspicious activity. EvaCam allows users to view both live and recorded video footage from cameras installed in their homes via a web server. Users can also receive email notifications whenever suspicious activity is detected by an analysis server. You have been hired as an engineering manager to oversee the development and production use of the software running on the camera, the web server and the analysis server. The camera hardware is built by another team, and the web server and analysis server are hosted by a major cloud provider.

- (a) List, with justification, the major technical components of the development environment you would commission to support your team of software engineers. [5 marks]
- (b) Describe a suitable example unit test, integration test and end-to-end test for EvaCam. [3 marks]
- (c) The senior management team demand your developers produce bug-free code and suggest this can be achieved by ensuring 100% code coverage with unit tests. Explain why this goal is unachievable and outline, with justification, an appropriate testing strategy. [7 marks]
- (d) Describe the key differences in any release process you might design for the EvaCam camera, web server and analysis server. [5 marks]

## SECTION D

## 7 Discrete Mathematics

- (a) Let  $n$  be a positive natural number. Show  $x \equiv y \pmod{n}$  determines an equivalence relation between integers  $x$  and  $y$ . [3 marks]
- (b) Describe the extended Euclid algorithm which given a pair of positive natural numbers  $(m, n)$  returns not only their gcd,  $\gcd(m, n)$ , but also its expression as a linear combination,  $j.m + k.n$ , for integers  $j$  and  $k$ . [7 marks]
- (c) Assume positive natural numbers  $m$  and  $n$  are coprime, so  $\gcd(m, n) = 1$  with associated linear combination  $j.m + k.n = 1$ , for integers  $j$  and  $k$ .

- (i) Show that for any natural numbers  $r$  and  $s$  there is a solution to

$$x \equiv r \pmod{m} \wedge x \equiv s \pmod{n}.$$

[Hint: Take  $x = s.j.m + r.k.n$ .] [4 marks]

- (ii) Show the solution is unique mod  $m.n$ , i.e.  $x \equiv y \pmod{m.n}$  for any two solutions  $x$  and  $y$ . [6 marks]

## 8 Discrete Mathematics

A binary relation  $\prec$  on a set  $A$  is *well-founded* iff there are no infinite descending chains  $\cdots \prec a_i \prec \cdots \prec a_1 \prec a_0$ .

- (a) Show a binary relation  $\prec$  on a set  $A$  is well-founded iff any nonempty subset  $Q$  of  $A$  has a minimal element, *i.e.* an element  $m$  such that

$$m \in Q \wedge \forall b \prec m. b \notin Q .$$

[5 marks]

- (b) Show that defining

$$(n_1, n_2) \prec (n'_1, n'_2) \Leftrightarrow (n_1, n_2) \neq (n'_1, n'_2) \text{ and } n_1 \leq n'_1 \text{ and } n_2 \leq n'_2$$

determines a well-founded relation between pairs of positive natural numbers.

[7 marks]

- (c) Let  $\longrightarrow$  be a binary relation between pairs of positive natural numbers for which

$$(m, n) \longrightarrow (m, n - m) \text{ if } m < n, \quad \text{and} \quad (m, n) \longrightarrow (m - n, n) \text{ if } n < m .$$

Using (a) and (b), or otherwise, show that for all pairs of positive natural numbers  $(m, n)$ , there is a natural number  $h$  such that

$$(m, n) \longrightarrow^* (h, h) .$$

[8 marks]

## 9 Discrete Mathematics

- (a) What does it mean for a function to be an injection, a surjection, and a bijection?  
[4 marks]
- (b) For sets  $A$  and  $B$ , define without proof a bijection from  $\mathcal{P}(A \times B)$  to  $[A \Rightarrow \mathcal{P}(B)]$  and its inverse.  
[4 marks]
- (c) For sets  $A$ ,  $B$  and  $C$ , define without proof a bijection from  $[(A \times B) \Rightarrow C]$  to  $[A \Rightarrow (B \Rightarrow C)]$  and its inverse.  
[4 marks]
- (d) Let  $X$  be a set. Prove there is no injection  $f : \mathcal{P}(X) \rightarrow X$ .  
[Hint: Consider the set  $W = \{f(Z) \mid Z \subseteq X \wedge f(Z) \notin Z\}$ .]  
[8 marks]

## 10 Discrete Mathematics

Consider formal languages  $L_{(x)}$  over the alphabet  $\Sigma = \{0, 1\}$ .

(a)  $L_{(a)} \subset \Sigma^*$  consists of all and only the strings with an even number of 0s.

(i) Build a regular expression for  $L_{(a)}$ . [2 marks]

(ii) Draw the transition graph of a deterministic finite automaton (DFA) for  $L_{(a)}$ . [2 marks]

(b)  $L_{(b)} \subset \Sigma^*$  is defined by the following axiom and rules:

$$\frac{}{0} \quad \frac{u}{001u} \quad \frac{w10u}{wu}$$

where  $u$  and  $w$  are string variables in  $\Sigma^*$  while 0 and 1 are literals.

(i) State a property  $P_1$  enjoyed by all strings in  $L_{(b)}$  but by none of the following strings: 01011, 1, 111, 11111100001100, 10101. [2 marks]

(ii) Prove that all strings in  $L_{(b)}$  enjoy the property  $P_1$  you defined in your answer to Part (b)(i). [3 marks]

(iii) Either prove the following statement or provide a counterexample: “There is no string in  $L_{(b)}$  with two consecutive 1s”. [4 marks]

(c) Language  $L_{(c)} \subset \Sigma^*$  consists of the strings that enjoy the following four properties simultaneously:

- $P_2$  : “having a number of 0s divisible by three”;
- $P_3$  : “including the 11011 substring”;
- $P_4$  : “having at least four 0s”;
- $P_5$  : “having no more than five 1s”.

(i) Give three minimum-length strings in  $L_{(c)}$ . [1 mark]

(ii) For each of the properties  $P_2$ – $P_5$ , draw the transition diagram for a matching DFA. [4 marks]

(iii) Describe how to build a DFA for  $L_{(c)}$  by combining the ones you built for Part (c)(ii). [2 marks]

**END OF PAPER**