COMPUTER SCIENCE TRIPOS Part IA

Tuesday 2 June 2020 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*) Use Boolean algebra to simplify the following functions:

$$X = \overline{A}.B.C + \overline{B.\overline{C}} + B.C$$
$$Y = \overline{(A + B + C)}.D + A.D + B$$

[6 marks]

(*b*) Implement the Boolean function

$$X = \overline{A}.\overline{B}.\overline{C} + B.\overline{C} + B.C$$

using

(*i*) an 8:1 Multiplexor;

(*ii*) a 4:1 Multiplexor, plus a NOT gate;

(*iii*) a 2:1 Multiplexor, plus a NOT gate, plus an OR gate.

[6 marks]

(*c*) A *priority encoder* has 2^N inputs. It produces an N-bit binary output indicating the most significant bit of the input that is TRUE, or 0 if none of the inputs is TRUE. It also produces an output NONE that is TRUE if none of the inputs is TRUE.

(*i*) Write down the Truth Table showing all inputs and all outputs for an eight-input priority encoder. [2 marks]

(*ii*) Give simplified Boolean expressions for all outputs of the eight-input priority encoder. [6 marks]

2 Digital Electronics

(a) With the aid of block and example state diagrams, describe the main features of Moore and Mealy implementations of finite state machines. [6 marks]

(b) A finite state machine (FSM) takes two inputs, A and B, and generates one output, Z. The output at cycle n, Z_n, is

$$Z_n = \begin{cases} A_n.A_{n-1} & \text{if } B_n = 0 \\ A_n + A_{n-1} & \text{if } B_n = 1. \end{cases}$$

(i) Determine the state transition table and the state diagram for a Mealy implementation of this FSM where the single D-type flip-flop state register has input A at its D-input. [5 marks]

(ii) Write down the Boolean functions for the next state and output combinational logic for the FSM. [2 marks]

(iii) Show how the FSM could be implemented using a 2:1 Multiplexor and some additional 2-input combinational logic gates. [2 marks]

(iv) Show how the FSM could be modified to eliminate the asynchronous changes on the output Z in response to inputs A and B. [1 mark]

(c) An FSM may be implemented using a generic logic array (GLA) device or a generic array logic (GAL) device. With the aid of diagrams, compare and contrast the architecture of GLA and GAL devices, specifically identifying the advantages and disadvantages of each device structure. [4 marks]

SECTION B

3 Operating Systems

Consider an operating system that uses hardware support for paging to provide virtual memory to applications.

(*a*) (*i*) Explain how the hardware and operating system support for paging combine to prevent one process from accessing another's memory. [3 marks]

(*ii*) Explain how space and time overheads arise from use of paging, and how the Translation Lookaside Buffer (TLB) mitigates the time overheads. [3 marks]

(*b*) Consider a system with a five level page table where each level in the page table is indexed by 9 bits and pages are 4 kB in size. A TLB is provided that is indexed by the first 57 bits of the address provided by the process, and achieves a 90% hit rate. A main memory access takes 40 ns while an access to the TLB takes 10 ns. The maximum memory read bandwidth is 100 GB/s.

(*i*) What is the effective memory access latency? [4 marks]

(*ii*) A colleague suggests replacing the system above with one that provides 80 GB/s memory read bandwidth and main memory access latency of 30 ns. Explain whether you should accept the replacement or not, and why. [4 marks]

(*c*) A creative engineer suggests structuring the TLB so that not all the bits of the presented address need match to result in a hit. Suggest how this might be achieved, and what might be the costs and benefits of doing so. [6 marks]

4 Operating Systems

An application processes network data at a constant rate of 1 MB/s. The data is transmitted at a long-term average rate of 1 MB/s but occasionally bursts at up to 5 MB/s for up to 2 s at a time.

(*a*) Why is it necessary for the operating system to provide some degree of buffering on behalf of the application? [2 marks]

(*b*) A rather simplistic operating system can only provide 1 MB sized buffers that cannot be simultaneously read and written. What will be the effect on the application if the systems only supports single buffering? [2 marks]

(*c*) A more advanced operating system provides double-buffering using 512 kB buffers that also cannot be simultaneously read and written. What impact does this have on the application? [3 marks]

(*d*) A further upgrade to the operating system uses 512 kB buffers to provide a circular buffer. How many buffers must be used to prevent the application experiencing data loss? [3 marks]

(*e*) A clever systems engineer proposes re-implementing the buffer so that it can be simultaneously read and written. Explain why they might propose this, what might be the challenges in doing so, and propose a simpler approach to achieve the same end. [5 marks]

(*f*) To switch between processes, the operating system must save the context of the currently executing process and restore the context of that being resumed. Explain how the relevant state is stored, and what it must contain. Explain why you would not include the IO buffers with that state. [5 marks]

SECTION C

5 Software and Security Engineering

You have been hired to design a mobile phone app for a brokerage firm, whose business is to help people to manage their investments. Their customers will use the app to check the prices of the shares and bonds that they own, sell them when they wish, and buy others. The customers' investment portfolios are typically worth six figures or more. You have already implemented industry standard mechanisms for the customer to authenticate to the app using the phone's biometric mechanisms, and for the app to authenticate itself to the broker's servers using TLS. Orders to sell investments, or to transfer sale proceeds from the customer's account at the brokerage to a bank account, also need a second authentication factor, as a requirement from the regulator. At present the brokerage sends an SMS message to the customer's phone.

The firm wants a recovery mechanism to support users who have lost their phone, bought a new one, and downloaded a new copy of the app. On initialisation, the app will generate a set of cryptographic keys, and send the public keys along with the phone's details to the broker, encrypted under the broker's TLS key. The recovery mechanism will authorise a new set of keys to be used to access an existing account and, together with the SMS second factor, to sell investments or withdraw the proceeds of sales.

(*a*) The brokerage firm first suggests sending an email to any customer who needs to recover an account, with an activation code to type into the app. Discuss the security, usability and cost of this option. [5 marks]

(*b*) Another suggestion is to rerun the initial 'know-your-customer' registration procedure which involves the customer sending the brokerage a photo of their passport or driving license plus two utility bills. Discuss the security, usability and cost of this option. [5 marks]

(*c*) Does the SMS second factor do any useful work? Justify your answer. [5 marks]

(*d*) What might you suggest that is better? Discuss its security, usability and cost. [5 marks]

6 Software and Security Engineering

(*a*) What is *fault tree analysis* ? [4 marks]

(*b*) What is *failure modes and effects analysis*? [4 marks]

(*c*) Discuss the likely shortcomings of failure modes and effects analysis with respect to *either* the Therac-25 accidents or the Boeing 737 Max accidents. [6 marks]

(*d*) Might the accidents have been avoided if the safety assessment had been based on fault tree analysis instead? [6 marks]

SECTION D

7 Discrete Mathematics

(*a*) Prove that, for all statements P and Q,

$$(P \implies Q) \implies \big((P \implies \neg Q) \implies \neg P\big)$$

[4 marks]

(*b*) (*i*) Let p and q be positive integers such that $\gcd(p, q) = 1$.

Prove that, for all integers a and b,

$$a \equiv b \pmod{p \cdot q} \iff \big(a \equiv b \pmod{p} \wedge a \equiv b \pmod{q}\big)$$

[5 marks]

(*ii*) State Fermat's Little Theorem. [3 marks]

(*iii*) Let p and q be distinct prime numbers and let e and d be natural numbers such that $e \cdot d \equiv 1 \pmod{(p-1)\cdot(q-1)}$.

Prove that, for all natural numbers n,

$$n^{e \cdot d} \equiv n \pmod{p \cdot q}$$

[8 marks]

8 Discrete Mathematics

(*a*) Let $\mathbb{N}_+ = \{\, \ell \in \mathbb{N} \mid \ell > 0 \,\}$.

(*i*) Prove that, for all $a, b \in \mathbb{N}_+$, if $a > b$ then $\gcd(a, b) = \gcd(a - b, b)$. [4 marks]

(*ii*) Prove the following statement for all $q \in \mathbb{N}_+$,

$$\forall\, n \in \mathbb{N}_+ \,.\, \forall\, r \in \mathbb{N}_+ \,.\; \gcd(2^{q \cdot n + r} - 1, 2^n - 1) = \gcd(2^r - 1, 2^n - 1)$$

[*Hint:* Proceed by induction on q]. [6 marks]

(*iii*) Prove that, for all $q, n \in \mathbb{N}_+$, $\gcd(2^{q \cdot n} - 1, 2^n - 1) = 2^n - 1$. [2 marks]

(*iv*) For $m, n \in \mathbb{N}_+$, give a formula for $\gcd(2^m - 1, 2^n - 1)$. Briefly justify your answer. [2 marks]

(*b*) Prove that there is no surjection from $\mathbb{N}$ to $\big(\mathbb{N} \Rightarrow \{0, 1\}\big)$. [6 marks]

9 Discrete Mathematics

(*a*) A partition of a set U is a family of sets $\mathcal{H} \subseteq \mathcal{P}(U)$ such that

- $\forall\, B \in \mathcal{H}.\ B \neq \emptyset$
- $\forall\, A, B \in \mathcal{H}.\ A \cap B \neq \emptyset \implies A = B$
- $U \subseteq \bigcup \mathcal{H}$

Prove that if $\mathcal{F}$ is a partition of a set A and $\mathcal{G}$ is a partition of a set B then

$$\mathcal{F} \otimes \mathcal{G} = \{\, Z \in \mathcal{P}(A \times B) \mid \exists\, X \in \mathcal{F}.\ \exists\, Y \in \mathcal{G}.\ Z = X \times Y \,\}$$

is a partition of the set $A \times B$. [6 marks]

(*b*) Let U be a set and $f : \mathcal{P}(U) \to \mathcal{P}(U)$ be a function such that

$$\forall\, X, Y \in \mathcal{P}(U)\,.\ X \subseteq Y \implies f(X) \subseteq f(Y)$$

Define $\mathcal{F} = \{\, Z \in \mathcal{P}(U) \mid f(Z) \subseteq Z \,\}$ and $\Phi = \bigcap \mathcal{F}$.

(*i*) Prove that $\Phi \in \mathcal{F}$. [4 marks]

(*ii*) Prove that $f(\Phi) \in \mathcal{F}$. [2 marks]

(*iii*) Prove that $f(\Phi) = \Phi$. [2 marks]

(*c*) Define without proof a bijection from $\mathbb{N}$ to $\{\, \mathtt{0}, \mathtt{1} \,\}^*$ and its inverse. [6 marks]

10 Discrete Mathematics

(a) Draw the state transition diagram of a deterministic finite automaton (DFA) that accepts language

$$L_1 = \left\{ x \in \{0,1\}^* \;\middle|\; \begin{array}{l} x \text{ is divisible by 8 if interpreted} \\ \text{as an unsigned binary integer} \end{array} \right\}.$$

Explain your construction. [6 marks]

(b) State whether

$$L_2 = \left\{ x \in \{\oplus, \ominus\}^* \;\middle|\; \text{no left substring of } x \text{ has more } \ominus\text{s than } \oplus\text{s} \right\}$$

(the "never in debt" language) is a regular language or not. Prove your answer. [8 marks]

(c) Consider language L_3 over the {A, B, C} alphabet, defined by the following inductive rules.

$$\frac{}{\mathtt{AB}}\ (0) \qquad \frac{\mathtt{A}x}{\mathtt{A}xx}\ (1) \qquad \frac{x\mathtt{BBB}y}{x\mathtt{C}y}\ (2) \qquad \frac{x\mathtt{CC}y}{xy}\ (3) \qquad \frac{x\mathtt{B}}{x\mathtt{BC}}\ (4)$$

(i) Produce three distinct derivations for string $\mathtt{ABB} \in L_3$. [3 marks]

(ii) Argue why $\mathtt{AC} \notin L_3$. [*Hint:* This is a difficult challenge and therefore even a good insight, rather than a full proof, might earn full marks.] [3 marks]

END OF PAPER