CST0
COMPUTER SCIENCE TRIPOS Part IA

Wednesday 5 June 2024 13:30 to 16:30

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) Show that the Boolean function F can be represented as the exclusive OR operation of two terms, where each term comprises the AND operation of 2 variables appearing in either complemented or uncomplemented form.

$$F(X, Y, Z) = X.Y \oplus \overline{X}.Z + Y.Z$$

[5 marks]

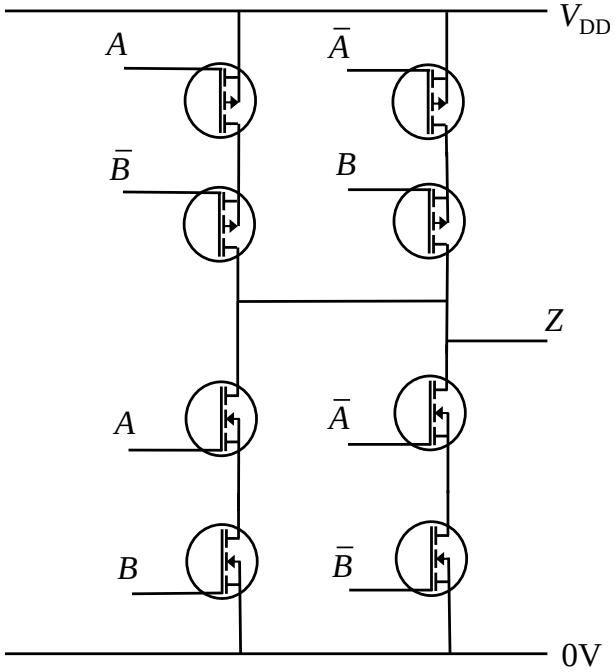
(b) Consider the Boolean function

$$G(A, B, C, D) = (A + B + \overline{C} + \overline{D}).(A + \overline{B} + C + D).(\overline{A} + \overline{B} + C).(\overline{A} + \overline{C} + \overline{D})$$

(i) Write down the minterms of G using decimal notation, where A represents the most-significant bit of the equivalent binary representation. [3 marks]

(ii) Simplify G into sum of products form using the Quine-McCluskey (Q-M) method. [7 marks]

(c) Briefly explain the operation of the following circuit and determine the Boolean function that relates the input variables, A and B, to the output Z? Assume that complemented input variables are available for use.



[5 marks]

2 Digital Electronics

(*a*) A synchronous 3-bit binary counter has a mode selection input X. If $X = 1$, the counter output sequence is 0, 1, 2, 3, 4, 5, 6, 7, 0, ... (decimal), and if $X = 0$, the counter output sequence is 7, 6, 5, 4, 3, 2, 1, 0, 7 ... (decimal). The counter is implemented using three, D type flip-flops with outputs labelled $\{Q_2, Q_1, Q_0\}$, where Q_0 represents the least significant bit.

(*i*) Write down the state transition table for this counter. [2 marks]

(*ii*) Detemine in simplified sum-of-products form, the next state combinational logic required for the D type flip-flops. [6 marks]

(*iii*) Show that the next state combinational logic for the D type flip-flop with output Q_1 can also be implemented using only exclusive OR (XOR) operations and a complement operation. [2 marks]

(*b*) A Mealy finite state machine (FSM) with input X and output Z is represented by the following state transition table.

Current state (Q)	Next state (Q')		Output (Z)	
	$X = 0$	$X = 1$	$X = 0$	$X = 1$
A	A	B	0	0
B	C	D	0	0
C	A	D	0	0
D	E	F	0	1
E	A	F	0	1
F	G	F	0	1
G	A	F	0	1

(*i*) Use row matching to eliminate states in this FSM and give the updated state transition table. [4 marks]

(*ii*) Show if this solution yields the minimum number of states. [2 marks]

(*c*) A D type flip-flop is used as a synchroniser to reduce problems owing to metastability in a synchronous FSM. P_{fail} is the probability of an invalid logic level at the synchroniser flip-flop output for a single input change and the input to the synchroniser flip-flop changes at a mean rate of N times/s.

(*i*) For $P_{fail} = 0.01$ and $N = 0.1$, what is the mean time between failure (MTBF) of the synchroniser?

(*ii*) Determine the minimum number of similar D type flip-flops that need to be cascaded for the synchroniser to achieve a minimum MTBF of 100 days?

[4 marks]

SECTION B

3 Operating Systems

(*a*) When an operating system needs to change a process' state from *ready* to *running* it does so by executing a *context switch*. What state must always be included in the context switch? What state must be flushed from the hardware before the new process is allowed to start running? [4 marks]

(*b*) A single-CPU system has five CPU-bound processes arrive simultaneously. Each has total CPU demand 10 ms, 20 ms, 30 ms, 40 ms, 50 ms respectively. Give the schedule by which processes are run and state how many context switches occur under the following scheduling regimes. Assume all processes have the default *nice* level.

(*i*) Round Robin, with a quantum of $q = 5$ ms.

(*ii*) Round Robin, with a quantum of $q = 20$ ms.

(*iii*) Completely Fair Scheduler, with a *target latency* of 60 ms, and a *minimum granularity* of 2 ms.

(*iv*) Completely Fair Scheduler, with a *target latency* of 20 ms, and a *minimum granularity* of 5 ms.

State which would be preferable for processing batch workloads, and which would be preferable for processing interactive workloads. Give a reason in each case. [10 marks]

(*c*) A modern-day cloud-provider decides to offer a service using Linux to which customers can deploy single *functions* as stand-alone units of computation. Their intention is that the relatively small size of such functions will give them more predictable behaviour, increasing customer satisfaction, as well as enabling instances to be packed more densely onto each physical machine, reducing the cloud-provider's costs. Suggest one reason why either assumption may fail, what effect that failure will have, and how the cloud-provider might try to ensure the assumption holds. [6 marks]

4 Operating Systems

(*a*) Address binding refers to the process of resolving memory references in a program to physical addresses when that program is brought into memory. Describe what is required for it to happen:

(*i*) At compile time

(*ii*) At load time

(*iii*) During execution

[3 marks]

(*b*) In a system containing three frames, consider the following string of page references:

1 2 3 2 4 3 5 1 3 2 3 4

Compute the sequence in which pages are allocated frames under the following algorithms:

(*i*) Optimal, OPT

(*ii*) Least Recently Used, LRU

(*iii*) First-In First-Out, FIFO

[9 marks]

(*c*) FIFO can exhibit *Bélády's anomaly*. State Bélády's anomaly, and explain why neither OPT nor LRU can exhibit it, but FIFO can. [4 marks]

(*d*) LRU is relatively expensive to implement, so some systems approximate it cheaply, determining which page to replace by using a *reference* bit and a *dirty* bit, respectively indicating whether a page was recently referenced or written to. A focused engineer wishes to implement such an LRU approximation on a machine that does not have hardware support for either reference or dirty bits. How might they emulate reference and dirty bits using paging hardware?

[4 marks]

SECTION C

5 Software and Security Engineering

The basic Europay-MasterCard-VISA transaction flow is

$$\begin{array}{ll} C \longrightarrow T: & PAN, d_1, \mathrm{Cert}_{KB}(PAN, d_1) \\ T \longrightarrow C: & N, t, X, d_2, PIN \\ C \longrightarrow T: & d_3, \mathrm{MAC}_{KCB}(d_3, T, N, t, X) \end{array}$$

where C is the customer card, T the merchant terminal, d_1 the card data, PAN the primary account number, N the unpredictable number, t the date, X the amount, d_2 and d_3 the merchant data, KB the bank signing key, KCB the key shared between the bank and the card and PIN the customer PIN.

(a) How does the merchant terminal obtain authorisation from the card-issuing bank? [4 marks]

(b) Describe two attacks on this protocol that can be used to commit fraud. In each case describe the protocol flaw or system limitation responsible. [8 marks]

(c) You are a security engineer working for a payment network owned by a country's banks. Which of the two attacks would most worry you, and what would you do to forestall or mitigate it? [8 marks]

6 Software and Security Engineering

You have joined a startup which plans to use a new solid state battery and a new electric motor to offer an improved auxiliary power kit for bicycles. The motor will fit in the front wheel hub and be connected to the battery by a cable. The battery will attach to the handlebar and the motor will be controlled by the a twist grip. In order to be legal, the motor must not power the bicycle at too high a speed. This speed limit is set by country but is typically 25, 30, 32 or 45 km/h.

(a) Using an appropriate methodology, list the combinations of actions that might lead to unsafe motor activation. [5 marks]

(b) Devise a safety policy and a security policy, and suggest a test strategy. [10 marks]

(c) What development methodology would you recommend? [5 marks]

SECTION D

7 Discrete Mathematics

You may use any standard results provided that you state them clearly.

(*a*) For a positive integer ℓ and an integer k, let $[k]_\ell$ denote the unique integer in $\mathbb{Z}_\ell$ congruent to k modulo ℓ.

For positive integers m and n, prove that if $[n]_m$ has a multiplicative inverse in $\mathbb{Z}_m$ then $[m]_n$ has a multiplicative inverse in $\mathbb{Z}_n$. [4 marks]

(*b*) (*i*) Calculate the greatest common divisor of 12346 and 57891. [4 marks]

(*ii*) (A) Define the greatest common divisor $\gcd(a, b)$ of two positive integers a and b. [2 marks]

(B) Prove that $\gcd\big(\gcd(a, b), c\big) = \gcd\big(a, \gcd(b, c)\big)$ for all positive integers a, b, c. [5 marks]

(*c*) Say whether the following statement is true or false, and respectively provide a proof or a counterexample justifying your claim.

For all sets X, $\mathcal{P}\big(X \uplus \{0\}\big) \cong \mathcal{P}(X) \uplus \mathcal{P}(X)$. [5 marks]

8 Discrete Mathematics

(*a*) Let $R \subseteq A \times B$ be a relation from a set A to a set B. For a subset $X \subseteq A$, define the subset $\mathrm{C}_R(X) \subseteq B$ as

$$\mathrm{C}_R(X) = \{\, b \in B \mid \forall\, a \in X.\ a\, R\, b \,\}$$

(*i*) Prove that, for all $P \subseteq Q \subseteq A$, one has $\mathrm{C}_R(Q) \subseteq \mathrm{C}_R(P)$. [2 marks]

Let $\mathcal{F} \subseteq \mathcal{P}(A)$ be a family of subsets of the set A.

(*ii*) Define the big intersection $\bigcap \mathcal{F} \subseteq A$ of $\mathcal{F}$. [2 marks]

(*iii*) Define the big union $\bigcup \mathcal{F} \subseteq A$ of $\mathcal{F}$. [2 marks]

(*iv*) Prove that $\mathrm{C}_R\big(\bigcup \mathcal{F}\big) = \bigcap \big\{\, Y \subseteq B \;\big|\; \exists\, X \in \mathcal{F}.\ Y = \mathrm{C}_R(X) \,\big\}$ [6 marks]

(*b*) Let A^* be the set of strings over an alphabet A.

Consider the subset W of A^* inductively defined by the following axiom and rule

$$\frac{}{\varepsilon} \qquad\qquad \frac{w}{w\,a}\ (a \in A)$$

(*i*) State the rule-induction proof method to show $\forall\, w \in W.\ P(w)$ for a property $P(w)$ of elements w of W. [2 marks]

(*ii*) Prove that $\forall\, w \in W.\ (\forall\, u, v \in A^*.\ w\,u = w\,v \implies u = v\,)$ by the rule-induction proof method. [6 marks]

9 Discrete Mathematics

(*a*) Let $f\colon A \to B$ be a function.

(*i*) What does it mean for a function $s\colon B \to A$ to be a ***section*** of the function $f\colon A \to B$? [2 marks]

(*ii*) What does it mean for a function $r\colon B \to A$ to be a ***retraction*** of the function $f\colon A \to B$? [2 marks]

(*b*) Let $f\colon A \to B$ be a function.

(*i*) Let $s\colon B \to A$ be a section of $f\colon A \to B$. Prove that any two sections $u, v\colon A \to B$ of $s\colon B \to A$ are equal. [2 marks]

(*ii*) Let $r\colon B \to A$ be a retraction of $f\colon A \to B$. Prove that any two retractions $u, v\colon A \to B$ of $r\colon B \to A$ are equal. [2 marks]

(*c*) We shall refer to a given function $f\colon A \to B$ as ***locally subsingleton*** when for every $b \in B$, the inverse image $f^{-1}\{b\} \subseteq A$ has *at most* one element, *i.e.* for any $x, y \in f^{-1}\{b\}$ we have $x = y$. Prove that a function $f\colon A \to B$ is *locally subsingleton* if and only if it is *injective*. [4 marks]

(*d*) We shall refer to a given function $f\colon A \to B$ as ***locally singleton*** when for every $b \in B$, the inverse image $f^{-1}\{b\} \subseteq A$ has *exactly* one element.

(*i*) Prove that any function $f\colon A \to B$ is *locally singleton* if and only if it is *bijective*. [4 marks]

(*ii*) Prove that the set of *bijective functions* from A to B is itself in bijection with the set of triples (f, g, h) with $f\colon A \to B$ and $g, h\colon B \to A$ such that g is a section of f and h is a retraction of f. You may use any standard results provided that you state them clearly. [4 marks]

10 Discrete Mathematics

(*a*) Let $\Sigma = \mathbb{N}$ be the alphabet whose symbols are given by natural numbers $0, 1, 2, \ldots$, and let L_n be the language over Σ consisting of finite strings of digits that sum to n.

(*i*) Draw a diagram of a DFA recognising L_3. [3 marks]

(*ii*) For arbitrary $n \in \mathbb{N}$, define a DFA $M_n = (Q_n, \Sigma, \Delta_n, s_n, F_n)$ over $\Sigma = \mathbb{N}$ that recognises the language L_n. [4 marks]

(*b*) Let $M = (Q, \Sigma, \Delta, s, F)$ be an NFA. We shall refer to M as ***complete*** when for any $q \in Q$ and $a \in \Sigma$, there exists some $q' \in Q$ such that $q \xrightarrow{a} q'$.

We shall refer to M as ***partially deterministic*** when for any states $q, q', q'' \in Q$ and input symbol $a \in \Sigma$, if both $q \xrightarrow{a} q'$ and $q \xrightarrow{a} q''$ then $q' = q''$ holds.

(*i*) Prove that an NFA is *deterministic* if and only if it is both *complete* and *partially deterministic*. [2 marks]

(*ii*) Suppose that M is a *partially deterministic* NFA; construct a DFA $M' = (Q', \Sigma, \Delta', s', F')$ over the same alphabet such that any finite string $u \in \Sigma^*$ is accepted by M if and only if it is accepted by M' and, moreover, such that the cardinality of Q' is bounded by $\#Q' < 2^{\#Q}$ assuming $\#Q > 1$. Argue that M' meets these requirements. [8 marks]

(*c*) Let $M = (Q, \Sigma, \Delta, s, F)$ and $M' = (Q', \Sigma, \Delta', s', F')$ be two DFAs over the same alphabet, writing $\delta \colon Q \times \Sigma \to Q$ and $\delta' \colon Q' \times \Sigma \to Q'$ for the next-state functions corresponding to the total functional relations Δ and Δ' respectively.

A ***homomorphism of DFAs*** from M to M', written $f \colon M \to M'$, is defined to be a function $f \colon Q \to Q'$ satisfying the following conditions:

- f preserves the starting state, *i.e.* $fs = s'$;
- f sends accepting states to accepting states, *i.e.* for $q \in F$ we have $fq \in F'$;
- f preserves transitions, *i.e.* $f(\delta(q, a)) = \delta'(f(q), a)$ for all $q \in Q$ and $a \in \Sigma$.

(*i*) Let $M_1 = (Q_1, \Sigma, \Delta_1, s_1, F_1)$ and $M_2 = (Q_2, \Sigma, \Delta_2, s_2, F_2)$ be two DFAs over Σ. Define a new DFA $M_1 \times M_2$ over Σ with states in the cartesian product $Q_1 \times Q_2$, such that the projections $\pi_1 \colon Q_1 \times Q_2 \to Q_1$ and $\pi_2 \colon Q_1 \times Q_2 \to Q_2$ form homomorphisms $\pi_1 \colon M_1 \times M_2 \to M_1$ and $\pi_2 \colon M_1 \times M_2 \to M_2$ of DFAs, with proof. [3 marks]

END OF PAPER