CST0
COMPUTER SCIENCE TRIPOS Part IA

Wednesday 11 June 2025 09:00 to 12:00

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 algebraically that the following functions can be implemented using either a 2-input exclusive OR gate or its complement.

(i) $F(X, Y) = X.Y \oplus (X + Y)$

(ii) $G(A, B) = A \oplus B \oplus (A + B) + \overline{A}.\overline{B}$

[4 marks]

(b) (i) Show how the following function may be implemented using an AND gate, an OR gate and an XOR gate, all having two inputs.

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

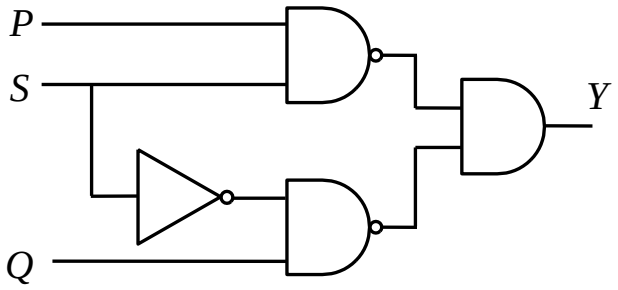
[3 marks]

(ii) Show how the function in Part (b)(i) may be implemented using a 16:1 multiplexer. Use variable A as the most significant bit of the multiplexer control inputs. [2 marks]

(iii) With the aid of a truth-table, show how the function in Part (b)(i) may alternatively be implemented using an 8:1 multiplexer and a NOT gate. Use variables A, B and C as the control inputs, where A is the most significant bit. Assume that complemented input variables are *not* available.

[4 marks]

(c) For the following circuit, assume that all the logic gates have an equal value of *non-zero* propagation delay and that $P = 1$ and $Q = 1$



(i) Describe what happens at output Y when input S changes from 1 to 0.

(ii) Show how the undesirable change observed at Y in Part (c)(i) may be removed.

[7 marks]

2 Digital Electronics

(a) The state transition table of a synchronous finite state machine (FSM) is

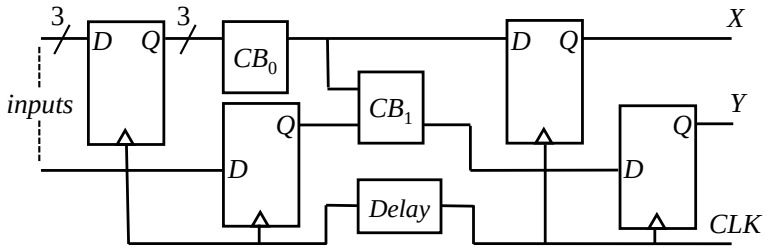
Current state	Next state				Output (Y)
	$X_1X_0 =$ 00	01	11	10	
S_0	S_0	S_1	S_1	S_1	0
S_1	S_0	S_0	S_2	S_2	1
S_2	S_0	S_0	S_3	S_0	1
S_3	S_0	S_0	S_0	S_0	1

(i) Assuming constant inputs over multiple clock cycles, determine the repeating bit sequence at Y for each of the four input combinations $X_1X_0 = \{00, 01, 11, 10\}$. The starting state does not matter. [4 marks]

(ii) Draw and label the state transition diagram for the FSM. [4 marks]

(iii) The FSM is to be implemented using two D-type flip-flops FF_1 and FF_0 having outputs Q_1 and Q_0 respectively. The state assignment is: $S_0[Q_1 = 0, Q_0 = 0]$, $S_1[Q_1 = 0, Q_0 = 1]$, $S_2[Q_1 = 1, Q_0 = 1]$ and $S_3[Q_1 = 1, Q_0 = 0]$. Determine the simplified equations necessary to generate the output Y and the flip-flop inputs D_1 and D_0. [5 marks]

(b) In the following schematic diagram, the *inputs* are connected to 4 D-type flip-flops (FFs) and CLK is the system clock. The outputs from 3 of the FFs are input to combinational logic block CB_0, and the output from the fourth FF is input to combinational logic block CB_1. The outputs from the combinational blocks are connected to two D-type FFs with outputs X and Y. For all FFs, the set-up time t_{su}= 50 ps, the hold time t_h= 60 ps, the propagation delay (clock-to-Q) t_{pc}= 80 ps and the minimum propagation delay (clock-to-Q) $t_{pc,min}$= 30 ps. For CB_0, the propagation delay t_{pd}= 80 ps and the minimum propagation delay $t_{pd,min}$= 50 ps. For CB_1, t_{pd}= 40 ps and $t_{pd,min}$= 25 ps. Unless stated otherwise, *Delay* has a propagation delay of t_{skew}= 0 ps.



(i) Determine the maximum clock frequency. [2 marks]

(ii) Determine if the FF hold time constraint is satisfied. [2 marks]

(iii) Now assume that t_{skew} = 20 ps. Determine the maximum clock speed, and whether the FF hold time constraint is now met. [3 marks]

SECTION B

3 Operating Systems

A UNIX system has three accounts: the standard *root* account plus three user accounts, *alice*, *bob*, and *chris*. The *access matrix* describes the various operations that different *domains* (also termed *subjects* or *principals*) can invoke on individual *objects*.

(*a*) In a large system, the access matrix may be very large but also very sparse. State the two common representations of the access matrix, and explain which you would use to represent access rights for a modern personal laptop.

[4 marks]

(*b*) The above UNIX system has four peripherals attached: a printer, a removable hard disk used for backups, a web camera with integral microphone, and a set of speakers. Give the access matrix corresponding to the following set of policy statements for the *read* and *write* operations on the four peripherals:

- *alice* may use the printer fully but *chris* may not use the printer at all, and *bob* may only check the printer's status.
- Only *root* may create backups and only *bob* may recover files from a backup.
- *alice* and *bob* are both allowed to participate fully in video-conferences, while *chris* may only play music.

[5 marks]

(*c*) Describe how an administrator might configure users, groups and file permissions on the system to create files with the following permissions:

(*i*) A file readable and writeable by *root* and *alice* and readable by *bob*.

(*ii*) A file readable and writeable by *root* and *bob* and readable by any user.

(*iii*) A file owned by *alice* but readable and writeable only by *root*.

[7 marks]

(*d*) A tidy-minded system administrator decides they would prefer all user IDs to count up from 1000. They start by changing the user ID of the *root* user from 0 to 1000. How does this change the access matrix for the files described in (*c*)? How will this impact administration of the system subsequently? [4 marks]

4 Operating Systems

Consider a 64 bit machine architecture providing 57 bit virtual addressing using linear-address translation with a five-level page table structure in which page table entries (PTEs) are 64 bits and a page is 4096 bytes.

(*a*) Using the largest applicable SI units, how much memory can be addressed using this scheme? [2 marks]

(*b*) Show how the virtual address `0x00c0.ffee.ba5e.f00d` is translated to a physical address using the five-level page table. As well as showing how each level in the page table structure is found and indexed, you should give the size of each level in the page table in terms of both bytes and entries, and give the full size of the page table. [9 marks]

(*c*) Assume that a memory access takes 40 ns, and the machine provides a Translation Lookaside Buffer (TLB) with a hit rate of 99% and a search time of 5 ns. What is the effective memory access time? [4 marks]

(*d*) An inspired engineer suggests replacing this five-level page table structure with a simple binary trie due to its expected $\log_2(N)$ lookup performance. State whether you would expect this to perform better or worse than the five-level page table structure, and explain why. [5 marks]

SECTION C

5 Software and Security Engineering

You have joined the team developing a new, rapidly growing social media service. The system is decentralised, in the sense that it allows anybody to run their own server and interact with users on other servers, e.g. by seeing posts made by users on other servers.

(*a*) Explain some possible strategies for testing the server software for this social network. [6 marks]

(*b*) Your server currently authenticates users via a password, but your team is discussing whether to introduce public key authentication. Discuss how this might work, and its pros and cons compared to passwords. Consider both how a user logs in to their home server, and also how posts on one server are authenticated by another server. [14 marks]

6 Software and Security Engineering

You have just launched your new band, where your role is to play the bagpipes and also act as the lead engineer of the website. Through a combination of talent and luck, the band has become an overnight sensation and you are now getting a huge surge of traffic to your site.

The band's website allows visitors to listen to your tracks, to purchase tickets for upcoming gigs and to sign up for your mailing list. However, you notice from the logs that a lot of visitors seem to browse the homepage and then leave without doing anything else.

(*a*) Describe how might you use behavioural analytics and experimental frameworks to increase engagement with your website. Give a concrete example that you work through in your answer. [6 marks]

(*b*) Explain the design and architecture of an A/B testing experimental framework that may be used to run experiments such as those you describe in part (*a*). [10 marks]

(*c*) The lyrics for your upcoming album are very politically sensitive, and listeners (both existing fans and new arrivals) may not want to reveal they are fans of you any more. What steps might you take to keep your fans safe and informed? Describe briefly also some limitations in what you can accomplish around online safety from just changes to your own website. [4 marks]

SECTION D

7 Discrete Mathematics

(a) (i) Say whether the statement below holds or not.

$$\begin{array}{l} \text{For all sets } A \text{ and } B\text{, relations } R \subseteq A \times B\text{, and subsets } S \subseteq B\text{,} \\ \qquad \forall\, b \in B.\ \big[\, \big(\exists\, a \in A.\ (a,b) \in R\big) \implies b \in S \,\big] \\ \iff \\ \qquad \forall\, y \in B.\ \big[\, \forall\, x \in A.\ \big((x,y) \in R \implies y \in S\big) \,\big] \end{array}$$

[2 marks]

(ii) Either prove or disprove the statement from Part(a)(i). [5 marks]

(b) Either prove or disprove the following statements.

(i) For all prime numbers p and integers n,

$$n^2 \equiv 1 \pmod{p} \implies \gcd(n,p) = 1$$

[3 marks]

(ii) For all prime numbers p and integers n,

$$\gcd(n,p) = 1 \implies n^2 \equiv 1 \pmod{p}$$

[3 marks]

(c) Let $\mathbb{N}$ be the set of natural numbers and let $\mathbb{B}$ be the set of bijections from $\mathbb{N}$ to $\mathbb{N}$.

Recall that two sets are said to be isomorphic whenever there is a bijection between them.

(i) Say whether or not $\mathbb{B}$ is isomorphic to $\mathbb{N} \times \mathbb{B}$. [2 marks]

(ii) Either prove or disprove that $\mathbb{B}$ and $\mathbb{N} \times \mathbb{B}$ are isomorphic. [5 marks]

(Hint: Consider that, for every $n \in \mathbb{N}$, the sets $\mathbb{N}$ and $\mathbb{N} \setminus \{n\}$ are isomorphic.)

8 Discrete Mathematics

(*a*) (*i*) Prove that for all positive integers m and integers n,

$$\gcd(n, m) = m \iff n \equiv 0 \pmod{m}$$

[2 marks]

(*ii*) Without using the Fundamental Theorem of Arithmetic, prove that for all prime numbers p and positive integers n,

$$\gcd(n, p) = 1 \iff n^{(p^2-1)} \equiv 1 \pmod{p}$$

[6 marks]

(*b*) Prove that the sum of the cubes of any three consecutive natural numbers is divisible by 9. [6 marks]

(*c*) Let $\mathcal{U} \subseteq \mathcal{P}(U)$ be a family of subsets of a set U such that, for all $\mathcal{F} \subseteq \mathcal{U}$, the big intersection $\bigcap \mathcal{F}$ is in $\mathcal{U}$.

Prove that, for all $\mathcal{F} \subseteq \mathcal{U}$, there exists a smallest element $\widehat{\mathcal{F}}$ of $\mathcal{U}$ that contains every element of $\mathcal{F}$ as a subset; that is,

(*i*) $\forall\, Y \in \mathcal{U}.\ (\forall\, X \in \mathcal{F}.\ X \subseteq Y\ ) \implies \widehat{\mathcal{F}} \subseteq Y$

(*ii*) $\forall\, Z \in \mathcal{F}.\ Z \subseteq \widehat{\mathcal{F}}$

[6 marks]

9 Discrete Mathematics

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

(*i*) Every injective function $m\colon A \hookrightarrow B$ has a retraction, *i.e.* a function $r\colon B \to A$ such that $r \circ m = \mathsf{id}_A$. [2 marks]

(*ii*) For all sets X and Y, if $\#X \leq \#Y$ then there exists a unique injective function $f\colon X \hookrightarrow Y$. [2 marks]

(*iii*) For all sets X and Y, if there exists an injective function $f\colon X \hookrightarrow Y$, then the cardinality of X is less than or equal to the cardinality of Y. [2 marks]

(*iv*) For all sets X and Y, if there exists a surjective function $f\colon X \twoheadrightarrow Y$, then the cardinality of X is greater than or equal to the cardinality of Y. [2 marks]

(*v*) For all sets X and Y, if there exist surjective functions $f\colon X \twoheadrightarrow Y$ and $g\colon Y \twoheadrightarrow X$, then X is isomorphic to Y. [1 mark]

(*b*) Prove that any subset of a countable set is countable. [3 marks]

(*c*) Let A be a finite set, so that $\#A = n$ for some $n \in \mathbb{N}$.

(*i*) What is the cardinality of the set $\mathrm{Rel}(A, A)$ of binary relations on A? [1 mark]

(*ii*) Let $\mathrm{RxRel}(A, A)$ denote the set of *reflexive* binary relations on A. (Recall that R is reflexive when $x\ R\ x$ for all $x \in A$.) Write down explicitly a function $\Phi\colon \mathrm{Rel}(A, A) \to \mathrm{RxRel}(A, A)$ that takes a relation S on A to the *smallest* reflexive relation on A containing S. Justify your answer with proof. [3 marks]

(*iii*) What is the cardinality of the set $\mathrm{RxRel}(A, A)$ of all reflexive binary relations on A? Justify your answer with proof. [4 marks]

10 Discrete Mathematics

(*a*) Let A be a set and let $R \subseteq A \times A$ be a binary relation on A. We define the *equivalence closure* of R to be the smallest equivalence relation $\sim_R \subseteq A \times A$ containing R as a sub-relation.

(*i*) Write down a set of *rules* over $A \times A$ that generate the equivalence closure of R in the sense that $x \sim_R y$ holds if and only if there exists a derivation with conclusion (x, y). (You must not use $\sim_R$; no proof is necessary.) [4 marks]

(*ii*) Write down a closed form definition of a set of relations $F \subseteq \mathcal{P}(A \times A)$ such that the intersection $\bigcap F$ is equal to $\sim_R$. (You must not use $\sim_R$.) Include a proof. [4 marks]

(*iii*) Let $E_R \subseteq A \times A$ be the relation defined so that $x \; E_R \; y$ holds if and only if there exists a derivation of (x, y) using the set of rules in the answer to Part (*a*)(*i*). Prove that E_R is equal to $\sim_R$. [4 marks]

(*b*) Let Σ and Q be finite sets. Give the cardinality of the set of deterministic finite automata over Σ with states in Q; note that two DFAs are the same when they have exactly the same sets of states, initial state, transition functions, and accepting states. Provide proof with your answer. [4 marks]

(*c*) Let Σ be a finite alphabet. Let L_p be the language consisting of all palindromes over Σ.

(*i*) Give a set of rules that inductively define L_p. [2 marks]

(*ii*) Write down a condition on the set Σ that holds if and only if L_p is regular. You may use any result proved in Lecture. [2 marks]

END OF PAPER