CST0
COMPUTER SCIENCE TRIPOS Part IA

Tuesday 8 June 2021   11:30 to 14:30 BST

COMPUTER SCIENCE Paper 2

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

*Submit each question answer in a **separate** PDF. As the file name, use your candidate number, paper and question number (e.g., `1234A-p2-q6.pdf`). Also write your candidate number, paper and question number at the start of each PDF.*

You must follow the official form and conduct instructions for this online examination

SECTION A

1 Digital Electronics

(*a*) Show that

(*i*) $(X+Y).(X+\overline{Y}) = X$

(*ii*) $(X+Y).(\overline{X}+Z) = (X+Y).(\overline{X}+Z).(Y+Z)$

[5 marks]

(*b*) With the help of the results in Part (*a*) or otherwise, simplify the following Boolean expression for W in to a product of sums (POS) form having 3 product terms, each having 3 literals

$$\begin{aligned} W \;=\; & (A+\overline{C}+\overline{F}+G).(A+\overline{C}+F+G).(A+B+\overline{C}+\overline{D}+G) \\ & .(A+C+E+G).(\overline{A}+B+G).(B+\overline{C}+F+G) \end{aligned}$$

[10 marks]

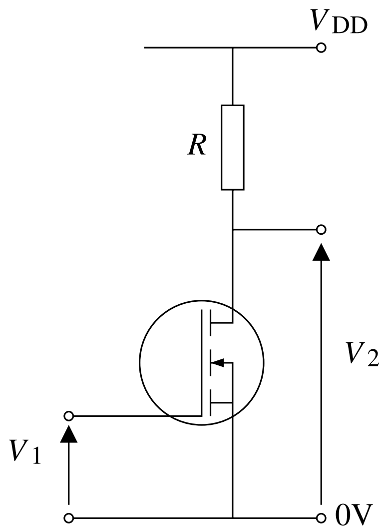
(*c*) (*i*) Using a Karnaugh map, simplify the following Boolean expression for V into a product of sums (POS) form

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

(*ii*) Implement the simplified expression for V obtained in Part (*c*)(*i*) using only NOR gates. Assume 2 and 4 input gates are available. Also assume complemented input variables are available. [5 marks]

2 Digital Electronics

The figure below shows a circuit using an N-channel MOSFET, along with a table giving the relationship between V_{DS} and I_{DS} for various values of V_{DS}, at $V_{\mathrm{DD}} = 4$ V and $V_{\mathrm{GS}} = 4$ V.



V_{DS}(mV)	160	320	470
I_{DS}(mA)	48	92	130

(*a*) Calculate the value of resistor R and the power dissipated in it when $V_{\mathrm{DS}} =$ 160 mV. [4 marks]

(*b*) A capacitor C is connected between the source and drain terminals of the MOSFET. After the MOSFET turns OFF at $t = 0$, the output signal V_2 as a function of time t is given by $V_2 = V_{\mathrm{DD}}(1 - e^{-t/CR})$. Assume that prior to $t = 0$, the MOSFET is ON and $V_2 = 0$ V.

(*i*) Determine an expression for the time taken t_r, for the output signal V_2 to rise from 20% to 80% of its maximum value.

(*ii*) What is the rise time t_r, if $C = 0.1\ \mu$F and R takes the value calculated in Part (*a*)?

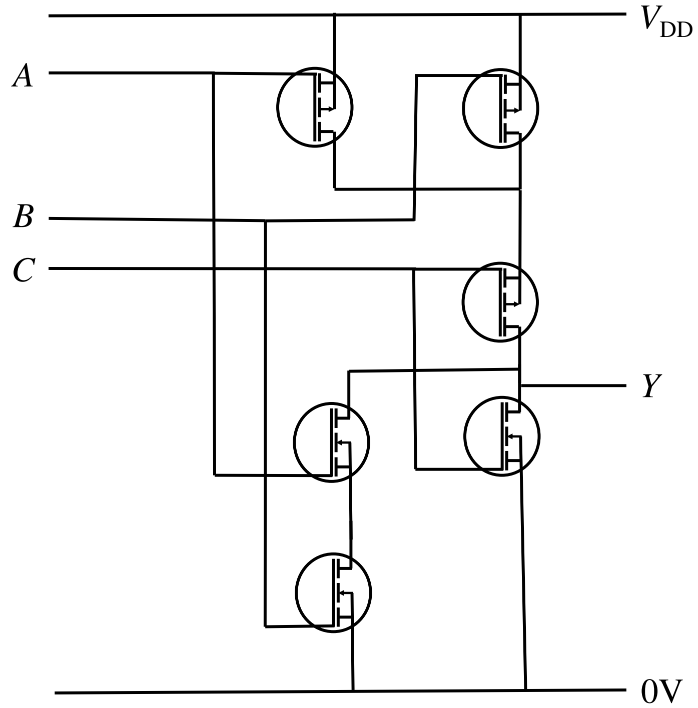
(*iii*) The value of R is changed so as to reduce the rise time to half that in Part (*b*)(*ii*). What is the new value of R?

(*iv*) Using the value of R calculated in Part (*b*)(*iii*), what is the power dissipated in R when the MOSFET is ON (i.e., when $V_{\mathrm{GS}} = 4$ V), and assuming that $V_2 = 320$ mV?

(*v*) Explain how the problem of high static power consumption seen in the N-channel MOSFET circuit can be eliminated. [9 marks]

[continued . . .]

(*c*) The logic gate in the following figure has 3 inputs, A, B, and C, and a single output Y. Determine the truth-table for the gate input to output function, and then determine a simplified Boolean expression for output Y in terms of A, B, and C.



[7 marks]

SECTION B

3 Operating Systems

(*a*) Assume a simple paging system with 2^{32} bytes of physical memory, 2^{48} bytes of logical address space and pages that are 2^{20} bytes in size. Further assume that each page table entry contains 4 bits indicating protection and validity of the entry.

(*i*) How many bits are used for the frame number and how many for the frame offset? [1 mark]

(*ii*) What is the total size of the page table in number of bits? [2 marks]

(*iii*) Assume that the working set of a typical process is fixed throughout the process lifetime and consists of 20 pages. How many entries would you suggest for the Translation Lookaside Buffer (TLB) for this system? What would its total size be in number of bits? Explain your answer. [4 marks]

(*iv*) Further assume that TLB search time is 20ns, TLB hit ratio is 80% and memory access time is 100ns. How many page table levels would you need to achieve an effective access time of 160ns, and why? [3 marks]

(*b*) (*i*) A Unix i-node has 12 disk addresses for direct disk blocks and three addresses for single, double, and triple indirect blocks. If each indirect block contains 256 disk addresses, what is the maximum file size supported by this system? Assume disk blocks of 4KB. [3 marks]

(*ii*) Assume that you are *user1* in a Unix file system and that you need to read the file `/home/user1/test/test1.html` which is stored in 4 disk blocks. Further assume that the `/` directory i-node is kept memory and each i-node and directory file fits in one disk block. How many disk accesses are required to read `test1.html`? Explain your answer. [4 marks]

(*iii*) Assume that *user1* wants to read `/home/user1/test/test2.html` immediately after reading `/home/user1/test/test1.html`. Further assume that file `test2.html` is stored in 4 disk blocks. How many disk accesses are required to read `test2.html`? Explain your answer. [3 marks]

4 Operating Systems

(*a*) Consider the following four processes to run in a single CPU. What is the average waiting time when scheduling these processes according to FCFS, SJF, and SRTF? [5 marks]

Process	Arrival Time	Burst Time
P1	0	8
P2	3	3
P3	5	4
P4	6	6

(*b*) Assume n processes in the READY queue. Discuss which scheduling algorithm(s) from FCFS, SJF, SRTF, and RR give(s) the minimum context switches for these n processes. Ignore any I/O burst. Explain your answer and clearly state your assumptions. [3 marks]

(*c*) Consider a computer with a CPU scheduler that implements the RR scheduling algorithm using a fixed time quantum that cannot be changed.

(*i*) Explain why RR provides a fair CPU allocation. [1 mark]

(*ii*) You need to give certain critical processes a greater share of the CPU without changing the scheduler. Describe how you could do so, and how your solution achieves this goal. [4 marks]

(*d*) Assume a Unix system with three users named `user1`, `user2`, and `user3`, and three groups named `group1`, `group2`, and `group3`. Assume `group1` has members `(user1, user2)`, `group2` has members `(user2, user3)`, and `group3` has members `(user3, user1)`. Consider three files with the following permissions:

```
rw-rw---- user1 group1 file1
rw-r--r-- user2 group3 file2
rwxr----- user3 group2 file3
```

(*i*) Which files can `user1` read? Which files can `user2` write? Which users can read `file3`? [3 marks]

(*ii*) `user2` cannot execute `file3`. What permissions does `file3` need so that all of its previous permissions are retained and `user2` can further execute this file? What permissions does `file3` need so that all of its previous permissions are retained and `user2` can further execute this file as `user3`? [4 marks]

SECTION C

5 Software and Security Engineering

A company has fired one of its senior staff after an incident that they claimed was an accident, but where the directors suspected malice. The company's auditors have suggested a review of the company's systems to mitigate 'the insider threat', and your advice has been sought. The directors want to be able to assure the shareholders that they are taking all reasonable steps to limit the damage that staff could do to affect the company's share price, whether accidentally or otherwise.

(*a*) Describe a multilevel security policy briefly, explaining what sort of harms it seeks to prevent, and how. [5 marks]

(*b*) Describe a separation-of-duty security policy briefly, explaining what sort of harms it seeks to prevent, and how. [5 marks]

(*c*) Describe one approach to minimising the risk of user error that is based primarily on psychology. [5 marks]

(*d*) Introducing architectural changes to the company's information systems will take time, while changes to user interfaces and workflows are often simple to implement. Which psychological approaches might be adopted more quickly, and what might you expect to go wrong? [5 marks]

6 Software and Security Engineering

A university has decided to implement a student monitoring system to enforce social distancing during the coronavirus pandemic. It is located in a country that does not expect to vaccinate all its residents until 2023, and the students will be about the last in line. As the budget is limited, the Vice-Chancellor plans to turn on event logging in its existing WiFi access points located in each lecture hall, lab and residence building to monitor that occupant numbers do not exceed notified limits. You may assume that access points can be configured to log network addresses, user logons or both.

(*a*) What performance, security and privacy issues might you expect? [7 marks]

(*b*) What policies might the Vice-Chancellor enact to manage the associated risks? [7 marks]

(*c*) Could you suggest any alternative strategies to the Vice-Chancellor? [6 marks]

SECTION D

7 Discrete Mathematics

(*a*) Without using the Fundamental Theorem of Arithmetic, prove that

$$\gcd(c, ab) = 1 \iff (\gcd(c, a) = 1 \wedge \gcd(c, b) = 1)$$

for all positive integers a, b, c. [5 marks]

(*b*) Let $P(n)$ be a statement for n ranging over the set of positive integers $\mathbb{N}^+$.

(*i*) Prove that if

$$\forall\, m \in \mathbb{N}^+.\ P(m+1) \implies P(m)$$

then

$$\forall\, n \in \mathbb{N}^+.\ P(n+1) \implies \big(\forall\, k \in \mathbb{N}^+.\ k \leq n+1 \implies P(k)\big)$$

[3 marks]

(*ii*) Prove that if

$$P(2) \wedge \big(\forall\, m \in \mathbb{N}^+.\ P(m) \Rightarrow P(2m)\big) \wedge \big(\forall\, m \in \mathbb{N}^+.\ P(m+1) \Rightarrow P(m)\big)$$

then

$$\forall\, n \in \mathbb{N}^+.\ P(n)$$

[3 marks]

(*c*) Let $I = \{\, x \in \mathbb{R} \mid 0 \leq x \leq 1 \,\}$.

In each case below define a function from I to I that satisfies the stated properties. Your answer should justify that the criteria are met.

(*i*) Injective but not bijective. [3 marks]

(*ii*) Surjective but not bijective. [3 marks]

(*iii*) Bijective but not the identity. [3 marks]

8 Discrete Mathematics

(a) Let i and j be positive integers.

(i) Prove that there exist natural numbers a and b such that $a \cdot i = b \cdot j + \gcd(i, j)$. You may use standard results provided that you state them clearly.

[4 marks]

(ii) Let m be a positive integer. Prove that, for all integers n,

$$\big(\, n^i \equiv 1 \pmod{m} \;\wedge\; n^j \equiv 1 \pmod{m} \,\big) \implies n^{\gcd(i,j)} \equiv 1 \pmod{m}$$

[3 marks]

(b) (i) For sets A and B, let $\approx$ be the binary relation on $(A \Rightarrow B)$ defined, for all $f, g \in (A \Rightarrow B)$, by

$$f \approx g \iff \exists\, \alpha \in \mathrm{Bij}(A, A).\, \exists\, \beta \in \mathrm{Bij}(B, B).\; \beta \circ f = g \circ \alpha$$

Prove that $\approx$ is an equivalence relation on $(A \Rightarrow B)$. [9 marks]

(ii) Recalling that, for $n \in \mathbb{N}$, we let $[n] = \{\, i \in \mathbb{N} \mid 0 \leq i < n \,\}$, define

$$S_n \;=\; \big(\,[n] \Rightarrow [2]\,\big)_{/\approx}$$

that is, the set S_n is the quotient of $\big(\,[n] \Rightarrow [2]\,\big)$ under the equivalence relation $\approx$.

(A) List the elements of S_n for each $n \in [4]$. [2 marks]

(B) What is the cardinality of S_n for each $n \in \mathbb{N}$? [2 marks]

9 Discrete Mathematics

(*a*) Prove that $4^n + 6n - 1 \equiv 0 \pmod 9$ for all natural numbers n. [5 marks]

(*b*) (*i*) State one of the standard characterizations of the reflexive-transitive closure $R^\star \subseteq A \times A$ of a binary relation R on a set A. [1 mark]

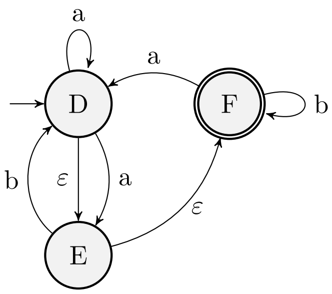
(*ii*) For the given characterization for a binary relation R on a set A, prove that $R^\star = \bigcup_{n\in\mathbb{N}} R_n$ where $R_0 = \emptyset$ and, for $n \in \mathbb{N}$, $R_{n+1} = \mathrm{id}_A \cup (R \circ R_n)$. You may use standard results provided that you state them clearly. [8 marks]

(*c*) Let $\mathcal{F} \subseteq \mathcal{P}(\mathbb{N})$ be a family of pairwise-disjoint subsets of natural numbers; that is, such that $\forall\, S, T \in \mathcal{F}.\ S \neq T \implies S \cap T = \emptyset$.

State whether or not the set $\mathcal{F}$ may be uncountable and prove your claim.
[6 marks]

10 Discrete Mathematics

(*a*) Consider the following NFA$^{\varepsilon}$, whose input alphabet is {a, b, c}.



(*i*) For each of the two strings abc and bba, state whether the automaton accepts it, with justification. [2 marks]

(*ii*) Using the subset construction, produce the full unoptimized state transition table of an equivalent DFA, *listing its states in lexicographic order* (important!) and indicating the starting and accepting states. [6 marks]

(*iii*) Give a regular expression, no longer than six symbols (metacharacters included), that describes the strings accepted by the automaton, together with an intuitive explanation for it. [*Hint:* Part (*a*)(*ii*) helps.] [4 marks]

(*b*) Consider language L_1 of strings over alphabet $\{0, 1\}$, defined inductively as follows.

$$\frac{}{\texttt{00}}\ (0) \qquad \frac{w}{\texttt{1}w}\ (1) \qquad \frac{w}{w\texttt{1}}\ (2)$$

(*i*) Draw the diagram of a DFA that recognizes L_1 in no more than four states. [4 marks]

(*ii*) Considering the words in L_1 as unsigned binary numerals, let language L_2 of strings over $\{0, 1\}$ be the set of all and only the binary numerals obtained by adding 1 to any numeral in L_1 and removing any leading zeros. NB: "adding" here means arithmetic addition, not string concatenation. Produce a regular expression no longer than 11 symbols that recognizes L_2, with a clear and convincing explanation of how you derived it. [4 marks]

END OF PAPER