COMPUTER SCIENCE TRIPOS Part IA

Tuesday 5 June 2018 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 minimise the following expressions. Give your answers in sum-of-products form.

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

(ii) $F = (A + B + \overline{C}).(A + B + D).(A + B + E).(A + \overline{D} + E).(\overline{A} + C)$

[8 marks]

(b) There may be more than one way of minimising a given Boolean expression into sum-of-products form. Demonstrate this by drawing a four-variable Karnaugh map that has two different minimised forms for the same Boolean expression, each with the same number of terms and literals. [4 marks]

(c) Simplify the following function $f(A, B, C, D, E)$ specified using the decimal representation of its minterms (where A represents the most significant bit of the equivalent binary representation) using the Quine-McCluskey (Q-M) method:

$$f(A, B, C, D, E) = \sum(0, 2, 3, 5, 7, 9, 11, 13, 14, 16, 18, 24, 26, 28, 30)$$

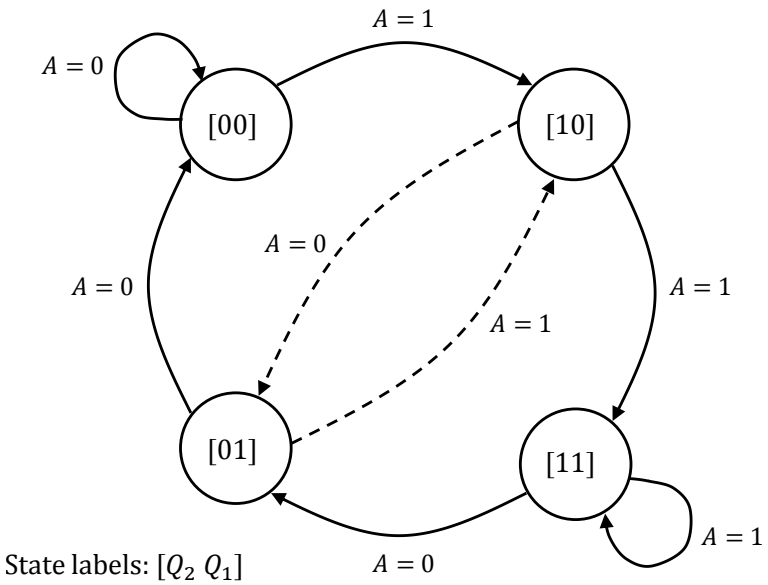
[8 marks]

2 Digital Electronics

(a) State the main features of a synchronous finite state machine (FSM) and describe its two main forms. [6 marks]

(b) With the aid of a diagram, show how a Transparent D-Latch can be implemented using cross-coupled NOR gates and some additional combinational logic. What are the advantages of the Transparent D-Latch over the RS latch? [6 marks]

(c) An FSM with input A has the function described in the following state diagram and is to be implemented using two synchronously clocked D-Type flip-flops as the state registers.



(i) Write down the corresponding state table taking into account all transitions in the state diagram, indicated by both solid and dashed lines. Show that the required FSM can be implemented by connecting the D-Type flip-flops in the form of a shift register.

(ii) For the implementation in Part (c)(i), what effect does increasing the clock rate of the D-Type flip-flops have on the likelihood of occurrence of the dashed-line transitions?

(iii) The two dashed-line transitions have the property of inverting Q_1. We now wish to replace both of them with transitions that occur under the same circumstances but instead have the property that Q_1 is unchanged. Give the four possible state diagrams satisfying this requirement and, for each state diagram, determine the next-state logic for the D-Type flip-flops.

[8 marks]

SECTION B

3 Operating Systems

(*a*) List four items of metadata that you might find in a *File Control Block (FCB)*. [4 marks]

(*b*) Consider a Unix process accessing a file using the standard API. Is protection provided through *Access Control Lists* or *Capabilities*? Justify your answer. [2 marks]

(*c*) Consider a filesystem structured as a directed acyclic graph (DAG) where files are structured from sets of 4096-byte disk blocks with 64-bit addresses. The first block of each file contains the following information:

control information:	1024 bytes
direct block pointers:	1008 bytes
indirect block pointer:	8 bytes
double indirect block pointer:	8 bytes
immediate data:	2048 bytes

The data bytes of a file start at the beginning of the immediate data. After the immediate data, the file data is found on the block addressed by the first direct block pointer and then carries on in a fashion similar to the structure defined by a Unix inode. We consider the first byte of the file to be byte 0, then byte 1, etc. Files are named by directory entries that are 128 bytes long. Directories are stored as files limited to a single block in size. Only two levels of directory are allowed. The root directory is stored in block 0.

You may find it useful to know that $126 * 8 = (2^7 - 2) * 2^3 = 1008$.

(*i*) Assuming identical structure for the first blocks of both files and directories, what is the maximum number of files this filesystem may contain? Without changing the size of a disk block, a disk block address, or a directory, how might you increase this, and to what? [4 marks]

(*ii*) How many disk blocks must be read to access byte 72 of a named file? How many must be read to access byte 2^{23}? [3 marks]

(*iii*) How big is the largest single file that can be stored in this filesystem? [3 marks]

(*iv*) Discuss the advantages and disadvantages of maintaining protection information with the file or with a directory entry for the file. [4 marks]

4 Operating Systems

(*a*) What is a *page fault*? [2 marks]

(*b*) How is a page fault handled if it is triggered by a process issuing a write for which it has permission on a machine with ample free memory at the point the page fault occurs? [6 marks]

(*c*) If the machine does not have sufficient free memory at the point that the page fault occurs, a *victim page* must be selected for replacement. Describe the ideal algorithm for handling this case, and explain why it cannot be implemented. [2 marks]

(*d*) Now describe a practical algorithm for selecting a victim page for replacement. In your answer you should discuss its performance, storage and time overheads, indicating any assumptions you make. [6 marks]

(*e*) What is *Bélády's Anomaly*? Can the algorithm described in Part (*d*) suffer from it? Justify your answer. (*Note*: You are not required to demonstrate an instance of Bélády's Anomaly occurring.) [4 marks]

SECTION C

5 Software and Security Engineering

(*a*) Although the following code compiles and executes without error, give four reasons why it is a poor test.

```
@Test
public void testIt() {
  long time = System.currentTimeMillis();
  double r = solve(40229321L);
  if (r < 1000.0) {
    assertThat(r == 430.6).isTrue();
  }
  long elapsed = System.currentTimeMillis() - time;
  assertThat(elapsed).isLessThan(3000);
}
```

[8 marks]

(*b*) You are running a project to develop the next version of an operating system that supports mandatory access control and limits the covert-channel bandwidth that a process at security level High can use to signal down to a process at security level Low.

Discuss the relative contribution of unit testing, integration testing and regression testing in checking that the covert-channel bandwidth is still acceptably low. [8 marks]

(*c*) The operating system is now going to be used in a different environment so that the load pattern will change. How might this affect covert-channel bandwidth? [4 marks]

6 Software and Security Engineering

A city council has decided to mount Bluetooth scanning equipment at each major road junction across the city and to use the information gathered to optimise traffic flows. In particular, it intends to control both the length of time for which specific traffic lights are green, and the relative timing of the green lights at different junctions. What performance, safety and security issues might arise, and what policies should be implemented to manage the associated risks? [20 marks]

Note: You should assume that the scanning equipment is able to obtain a unique network address for the majority of vehicles and of smartphones carried by cyclists moving through the city. The scanning equipment does not contain any exploitable vulnerabilities but you may assume that an attacker can simulate the existence of many Bluetooth devices from a single smartphone located near a scanner.

SECTION D

7 Discrete Mathematics

(*a*) Find all solutions in $\mathbb{Z}_{187}$ of the following congruence

$$x^2 + 5x + 6 \equiv 0 \pmod{187}$$

Justify your answer. [6 marks]

(*b*) For $\ell \in \mathbb{N}$, let $[\ell] = \{i \in \mathbb{N} \mid i < \ell\}$.

(*i*) Prove that, for all $\ell, m \in \mathbb{N}$, $[m] \times [\ell] \cong [m \cdot \ell]$ [3 marks]

(*ii*) Prove that, for all $\ell, m \in \mathbb{N}$, $[m] \uplus [\ell] \cong [m + \ell]$ [3 marks]

(*iii*) For $m, n \in \mathbb{N}$, define $\oplus$ by

$$[m] \oplus [0] = [m] \quad \text{and} \quad [m] \oplus [n+1] = \big([m] \oplus [n]\big) \uplus [1]$$

Prove that, for all $\ell, m \in \mathbb{N}$,

$$[m] \oplus [\ell] \cong [\ell] \oplus [m]$$ [8 marks]

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

8 Discrete Mathematics

(*a*) Let $R \subseteq X \times Y$ and $P \subseteq Y$ for sets X and Y.

Prove that

$$\forall\, y \in Y.\ \Big(\ \big[\,(\exists\, x \in X.\ x\,R\,y) \Rightarrow y \in P\,\big] \iff \big[\,\forall\, x \in X.\ (x\,R\,y \Rightarrow y \in P)\,\big]\ \Big)$$

[6 marks]

(*b*) Define the notions of

(*i*) injective function between two sets [1 mark]

(*ii*) surjective function between two sets [1 mark]

(*c*) Let $\mathbb{N}_+ = \{n \in \mathbb{N} \mid n > 0\}$ and define the function $e : \mathbb{N} \times \mathbb{N} \to \mathbb{N}_+$ by

$$e(m, n) = 2^m(2n + 1)$$

Without using the Fundamental Theorem of Arithmetic, prove that e is

(*i*) injective [4 marks]

(*ii*) surjective [8 marks]

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

9 Discrete Mathematics

(*a*) Define $F_0 = 0$, $F_1 = 1$ and for $n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$.

For positive integers a and b, prove that

$$\forall\, n \in \mathbb{N}.\ \gcd(aF_{n+3} + bF_{n+2},\, aF_{n+1} + bF_n) = \gcd(a, b) \qquad \text{[7 marks]}$$

(*b*) Let U be a set and let $\mathcal{P}(U)$ denote its powerset.

For $\mathcal{F} \subseteq \mathcal{P}(U)$, define $\mathcal{G} \subseteq \mathcal{P}(U)$ as $\{X \subseteq U \mid \forall\, S \in \mathcal{F}.\ S \subseteq X\}$.

Prove that $\bigcup \mathcal{F} = \bigcap \mathcal{G}$. [4 marks]

(*c*) For $i = 0, 1$, let $M_i = (Q_i, \Sigma, \delta_i, s_i, F_i)$ be deterministic finite automata, where $\delta_i : Q_i \times \Sigma \to Q_i$ are the next-state functions.

A relation $R \subseteq Q_0 \times Q_1$ is said to be a *simulation* whenever

$$\begin{array}{l} \forall\, q \in Q_0, q' \in Q_1. \\ \quad q\, R\, q' \implies \left[\ (q \in F_0 \Rightarrow q' \in F_1) \wedge \forall\, a \in \Sigma.\ \delta_0(q, a)\, R\, \delta_1(q', a)\ \right] \end{array}$$

(*i*) For $i = 0, 1$, let $\delta_i^{\#} : Q_i \times \Sigma^* \to Q_i$ be defined, for $q \in Q_i$, $a \in \Sigma$ and $w \in \Sigma^*$, by

$$\begin{array}{rcl} \delta_i^{\#}(q, \varepsilon) & = & q \\ \delta_i^{\#}(q, aw) & = & \delta_i^{\#}(\delta_i(q, a), w) \end{array}$$

For a simulation $R \subseteq Q_0 \times Q_1$, prove that

$$\forall\, w \in \Sigma^*.\ \forall\, q \in Q_0, q' \in Q_1.\ q\, R\, q' \implies \delta_0^{\#}(q, w)\, R\, \delta_1^{\#}(q', w) \qquad \text{[7 marks]}$$

(*ii*) For $i = 0, 1$, define $L(M_i) = \{w \in \Sigma^* \mid \delta_i^{\#}(s_i, w) \in F_i\}$.

Prove that if there exists a simulation $R \subseteq Q_0 \times Q_1$ such that $s_0\, R\, s_1$ then $L(M_0) \subseteq L(M_1)$. [2 marks]

10 Discrete Mathematics

(*a*) Let $\Sigma = \{a, b\}$ and let $\#_x(w)$ be the number of occurrences of the symbol $x \in \Sigma$ in the string w. For each of the following determine, with justification, whether or not the language is regular.

(*i*) $L_1 = \{w \in \Sigma^* \mid \#_a(w) = \#_b(w)\}$ [3 marks]

(*ii*) $L_2 = \{w \in \Sigma^* \mid w$ has an equal number of occurrences of the substrings ab and $ba\}$. [3 marks]

(*iii*) L_3 inductively defined by the following axiom and rule:

$$\frac{}{\epsilon} \qquad \frac{u}{aub} \qquad \text{for all } u \in \Sigma^*$$ [3 marks]

(*iv*) L_4 inductively defined by the following axiom and rules:

$$\frac{}{\epsilon} \qquad \frac{u}{aub} \qquad \frac{u}{au} \qquad \frac{u}{ub} \qquad \text{for all } u \in \Sigma^*$$ [3 marks]

(*v*) $L_5 = \{w \in \Sigma^* \mid (\#_a(w) = 3i) \wedge (\#_b(w) = 7j)$ for some $i, j \in \mathbb{N}\}$ [3 marks]

(*b*) Consider the set R of all regular expressions over the alphabet $\{a, b\}$.

(*i*) Give an alphabet sufficient to express any element of R. [2 marks]

(*ii*) State, giving reasons, whether R is a regular language. [3 marks]

END OF PAPER