COMPUTER SCIENCE TRIPOS Part IA

Thursday 8 June 2017 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*) Briefly describe the main feature of a combinational logic block. [2 marks]

(*b*) Use Boolean algebra to simplify the following expression

$$W = A.\overline{B}.C.\overline{D}.E + A.C.D + A.C.\overline{F}.G.\overline{H} + A.B.C.\overline{D}.E + A.C.D.\overline{E} + \overline{E}.\overline{H}$$

in sum of products form.

Hint: $X.Y + \overline{X}.Z = X.Y + \overline{X}.Z + Y.Z$ [4 marks]

(*c*) A 2-bit binary adder sums two numbers, A_1A_0 and B_1B_0 to yield the unsigned result $Y_2Y_1Y_0$, where the zero subscript indicates the least significant bit (LSB).

(*i*) Write down the truth table for the required outputs Y_2, Y_1 and Y_0.

(*ii*) Using a Karnaugh map (K map) or otherwise, give the simplified sum of products expression for Y_2.

(*iii*) Using a K map or otherwise, determine a simplified product of sums expression for Y_2 and show how the circuit can be implemented using only NOR gates (of any number of inputs).

[7 marks]

(*d*) Simplify the following four variable function $F(A, B, C, D)$ using the Quine-McCluskey (Q-M) method:

Minterms: $\overline{A}.\overline{B}.\overline{C}.\overline{D}$, $\overline{A}.\overline{B}.C.D$, $\overline{A}.B.\overline{C}.D$, $\overline{A}.B.C.D$, $A.\overline{B}.\overline{C}.\overline{D}$, $A.\overline{B}.C.\overline{D}$

Don't cares: $\overline{A}.\overline{B}.\overline{C}.D$, $A.\overline{B}.\overline{C}.D$, $A.B.C.D$ [7 marks]

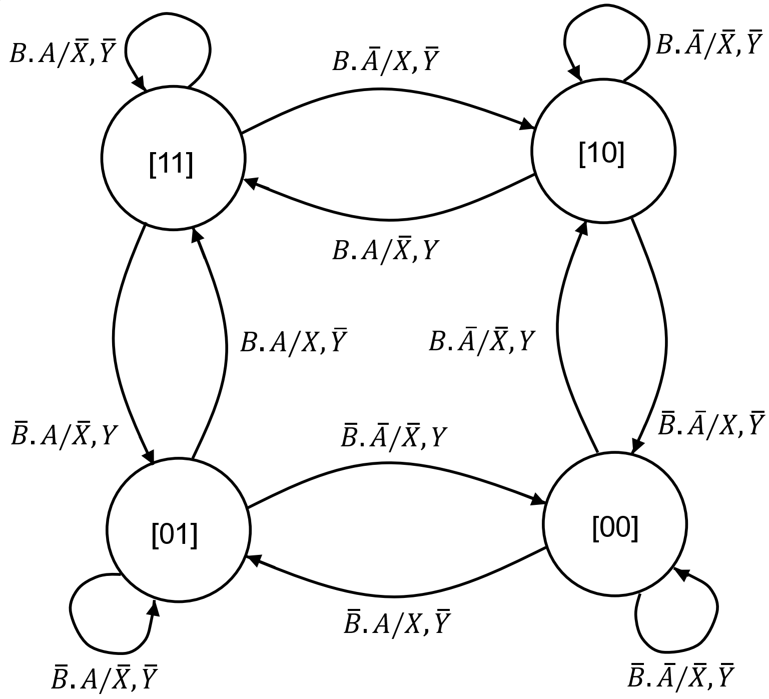
2 Digital Electronics

(*a*) Give the truth table for an RS Latch implemented using two cross coupled NOR gates and determine the state diagram for the $\overline{Q}$ output. [6 marks]

(*b*) Give the truth table for a 2-to-4 decoder (i.e., 2 control inputs, S_1, S_0, and 4 outputs, Q_3, Q_2, Q_1, Q_0) and show how it can be implemented using 2-input NOR and NOT gates. [4 marks]

(*c*) Show how the 2-to-4 decoder in part (*b*) can be used to implement a 4-to-1 multiplexor (i.e., 4 inputs, 2 control inputs and 1 output) using only NAND gates for the additional combinational logic required. [4 marks]

(*d*) (*i*) Write down the state transition table corresponding to the following state diagram



where $[Q_B\,Q_A]$ are the current state, B and A are the inputs, and X and Y are the outputs.

(*ii*) Show how two *D-type flip flops* and two *4-to-1 multiplexors* can be used to implement the Mealy machine given in the state diagram in part (*d*)(*i*).

[6 marks]

SECTION B

3 Operating Systems

(*a*) What is the *CPU IO burst cycle*? How does it motivate *multi-programming*? What does it mean for a process to be *CPU bound* or *IO bound*? [6 marks]

(*b*) Consider a single processor system supporting two running processes, A and B, with the following sequential execution patterns:

A: [CPU 8 ms; IO 1 ms; CPU 8 ms; IO 1 ms; CPU 8 ms]
B: [CPU 2 ms; IO 1 ms; CPU 2 ms; IO 1 ms; CPU 2 ms]

Assume that IO operations do not interfere with each other and are blocking, and that scheduling and context switch times are negligible.

(*i*) What is the total elapsed time for the two processes to run to completion? [2 marks]

(*ii*) Assume the system runs a non-preemptive scheduler where processes are scheduled in the order in which they become runnable, and that B takes priority over A in the event of a tie. Give the combined execution pattern of the two processes in the format as in part (*b*), and determine the total elapsed time for the two processes to run to completion. [5 marks]

(*iii*) Repeat part (*b*)(*ii*) with a pre-emptive scheduler operating with a time slice of 4 ms. [5 marks]

(*iv*) What are the costs and the benefits of a pre-emptive over a non-preemptive scheduler for this workload, which would you choose, and why? [2 marks]

4 Operating Systems

(*a*) The operating system typically provides each process with the illusion that it runs in a contiguous piece of memory. State the problem of *external fragmentation* in memory where processes have variably sized memory partitions. Describe how *paged virtual memory* solves this problem, and any time and space costs it introduces. [4 marks]

(*b*) Consider a 64 bit machine architecture providing 48 bit virtual addressing where the operating system uses a 4-level page table structure where a page is 4096 bytes and each page table entry is 8 bytes in size.

(*i*) Show how the virtual address `0x00be.efc0.ffee` is mapped to a physical address using the 4-level page table. You should give the size of each level in the page table in terms of both bytes and entries, as well as the size of a page table. [6 marks]

(*ii*) Assume a memory access takes 40 ns, and the machine provides a Translation Lookaside Buffer (TLB) with a hit rate of 90% and a search time of 10 ns. What is the effective memory access time? [4 marks]

(*iii*) Assume that a naive operating system designer instead proposes to use only a single level of page table structure. Show how this will affect both the space overheads of paging and the effective memory access time. Indicate whether a single level of page table is practical in this system. [3 marks]

(*c*) Consider a system where each process has three distinct memory areas requiring distinct access permissions. How do the space and time overheads due to paging change if the system moves from using small (e.g., 2^{12} byte) pages to using large (e.g., 2^{22} byte) pages? [3 marks]

SECTION C

5 Software and Security Engineering

The public-key Needham-Schroeder protocol is as follows:

$$\begin{aligned} A &\longrightarrow B : \{NA, A\}_{KB} \\ B &\longrightarrow A : \{NA, NB\}_{KA} \\ A &\longrightarrow B : \{NB\}_{KB} \end{aligned}$$

(*a*) Explain the notation used and the purpose of the protocol. [4 marks]

(*b*) What is wrong with this as a protocol design and how might this flaw be fixed? [10 marks]

(*c*) What would we still have to check about an implementation? [6 marks]

6 Software and Security Engineering

(*a*) Explain the difference between redundancy, backup and fallback. [4 marks]

(*b*) Give an example of a failure that cannot be mitigated by backup. [4 marks]

(*c*) Give two examples of systems where managing redundancy is easy, and two where it is hard. [8 marks]

(*d*) Can you suggest one or more general principles for distinguishing the cases in part (*c*) above? [4 marks]

SECTION D

7 Discrete Mathematics

(*a*) (*i*) Calculate $\gcd(144, 77)$, the greatest common divisor of 144 and 77, as an integer linear combination of 144 and 77. [4 marks]

(*ii*) What is the multiplicative inverse of 77 in $\mathbb{Z}_{144}$ and the multiplicative inverse of 67 in $\mathbb{Z}_{77}$? [2 marks]

(*iii*) Describe all integers x that solve the following two congruences

$$\begin{cases} 77 \cdot x \equiv 1 \pmod{144} \\ 67 \cdot x \equiv 3 \pmod{77} \end{cases}$$

Indicate how one may calculate the least natural number solution to the above. [4 marks]

Justify your answers.

(*b*) For a string $w \in \{1,2\}^*$, let $\sum(w) \in \mathbb{N}$ denote the sum of all the numbers in it. For instance, $\sum(\varepsilon) = 0$ for ε the null string, and $\sum(1212) = 6$.

For every $n \in \mathbb{N}$, define $S_n = \big\{ w \in \{1,2\}^* \mid \sum(w) = n \big\}$. In particular, $\varepsilon \in S_0$ and $1212 \in S_6$.

(*i*) List the elements of S_n for each $n \in \{0, 1, 2, 3, 4, 5\}$. [2 marks]

(*ii*) What is the cardinality of S_n for each $n \in \mathbb{N}$? Prove your claim. [5 marks]

(*iii*) For all $m, n \in \mathbb{N}$, define a bijective function

$$\big((S_{m+1} \times S_{n+1}) \uplus (S_m \times S_n)\big) \to S_{m+n+2}$$ [3 marks]

8 Discrete Mathematics

(*a*) For a non-empty tuple of positive integers $a_1, \ldots, a_n$, let

$$\mathrm{CD}(a_1, ..., a_n) \;=\; \{\, d \in \mathbb{N} \,:\, \forall\, 1 \leq i \leq n.\; d \mid a_i \,\}$$

be the set of natural numbers that are common divisors of all $a_1, \ldots, a_n$.

(*i*) Without using the Fundamental Theorem of Arithmetic, prove that for positive integers a and a', if $\mathrm{CD}(a, a') = \{1\}$ then, for all integers k,

$$(a \cdot a') \mid k \iff a \mid k \,\wedge\, a' \mid k$$

[4 marks]

(*ii*) Either prove or disprove that, for all natural numbers $n \geq 2$ and all tuples of positive integers $a_1, \ldots, a_n$, if $\mathrm{CD}(a_1, \ldots, a_n) = \{1\}$ then, for all integers k, $(a_1 \cdot \ldots \cdot a_n) \mid k \implies a_1 \mid k \,\wedge\, \ldots \,\wedge\, a_n \mid k$. [3 marks]

(*iii*) Either prove or disprove that, for all natural numbers $n \geq 2$ and all tuples of positive integers $a_1, \ldots, a_n$, if $\mathrm{CD}(a_1, \ldots, a_n) = \{1\}$ then, for all integers k, $a_1 \mid k \,\wedge\, \ldots \,\wedge\, a_n \mid k \implies (a_1 \cdot \ldots \cdot a_n) \mid k$. [3 marks]

(*b*) Either prove or disprove that for all sets A, B, X, Y,

$$(\, A \cong X \,\wedge\, B \cong Y \,) \implies A \times B \;\cong\; Y \times X$$

[4 marks]

(*c*) (*i*) Define the notion of a surjective function between two sets. [2 marks]

(*ii*) State whether or not the function $f : \mathbb{N} \to \{n \in \mathbb{N} \mid n \geq 1\}$ defined by

$$f(0) = 1$$

$$f(n+1) = \begin{cases} f(n)/2 & \text{if } f(n) \text{ is even} \\ 9 \cdot f(n) + 1 & \text{otherwise} \end{cases} \qquad (n \in \mathbb{N})$$

is surjective. Prove your claim. [4 marks]

9 Discrete Mathematics

(*a*) Let r and s be solutions to the quadratic equation $x^2 - b\,x + c = 0$.

For $n \in \mathbb{N}$, define

$$\begin{aligned} d_0 &= 0 \\ d_1 &= r - s \\ d_n &= b\,d_{n-1} - c\,d_{n-2} \quad (n \geq 2) \end{aligned}$$

Prove that $d_n = r^n - s^n$ for all $n \in \mathbb{N}$. [4 marks]

(*b*) Recall that a commutative monoid is a structure $(M, \mathtt{1}, *)$ where M is a set, $\mathtt{1}$ is an element of M, and $*$ is a binary operation on M such that

$$x * \mathtt{1} = x \quad , \quad x * y = y * x \quad , \quad (x * y) * z = x * (y * z)$$

for all x, y, z in M.

For a commutative monoid $(M, \mathtt{1}, *)$, consider the structure $(\mathcal{P}(M), I, \circledast)$ where $\mathcal{P}(M)$ is the powerset of M, I in $\mathcal{P}(M)$ is the singleton set $\{\mathtt{1}\}$, and $\circledast$ is the binary operation on $\mathcal{P}(M)$ given by

$$X \circledast Y = \{\, m \in M \mid \exists\, x \in X.\ \exists\, y \in Y.\ m = x * y \,\}$$

for all X and Y in $\mathcal{P}(M)$.

Prove that $(\mathcal{P}(M), I, \circledast)$ is a commutative monoid. [10 marks]

(*c*) Define a section-retraction pair to be a pair of functions $(s : A \to B, r : B \to A)$ such that $r \circ s = \mathrm{id}_A$.

(*i*) Prove that for every section-retraction pair (s, r), the section s is injective and the retraction r is surjective. [4 marks]

(*ii*) Exhibit two sets A and B together with an injective function $f : A \to B$ such that there is no function $g : B \to A$ for which (f, g) is a section-retraction pair. [2 marks]

10 Discrete Mathematics

For each of the following languages over the alphabet $\{a, b\}$, state with justification whether the language is regular or not. m and n are natural numbers.

(*a*) L_1 is the set of all strings with the number of a's in each being divisible by 3 and the number of b's being divisible by 7. [4 marks]

(*b*) $L_2 = \{a, b\}$ [4 marks]

(*c*) $L_3 = \{a^m b^n \mid m \neq n\}$ [4 marks]

(*d*) $L_4 = \{uww^R v$ for nonempty strings $u, w, v \in \{a, b\}^*\}$

w^R is the string obtained by reversing the string w. [4 marks]

(*e*) $L_5 = \{a^n \mid \text{where there are twin primes } p, p + 2, \text{ with } p > n\}$

Twin primes are pairs of primes which differ by 2, such as 5 and 7, or 17 and 19. It has been conjectured – but never proven – that there are infinitely many twin primes. [4 marks]

END OF PAPER