COMPUTER SCIENCE TRIPOS Part IA

Tuesday 5 June 2007 1.30 to 4.30

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
None

SECTION A

1 Digital Electronics

(a) State De Morgan's theorems. [4 marks]

(b) Simplify the function

$$f = \bar{a}\bar{b}\bar{c}\bar{d} + \bar{a}b\bar{c}d + a\bar{b}\bar{c} + a\bar{b}\bar{d}$$

with don't care states $\bar{a}\bar{b}\bar{c}d$ and $\bar{a}\bar{b}c\bar{d}$ to give expressions in the following forms:

(i) sum of products; [3 marks]

(ii) product of sums. [3 marks]

(c) Simplify the function

$$f = (\bar{a} + \bar{b} + \bar{c}).(b + d)$$

to give an expression in the sum of products form. [6 marks]

(d) Implement with 2-level logic the function in part (c) using only

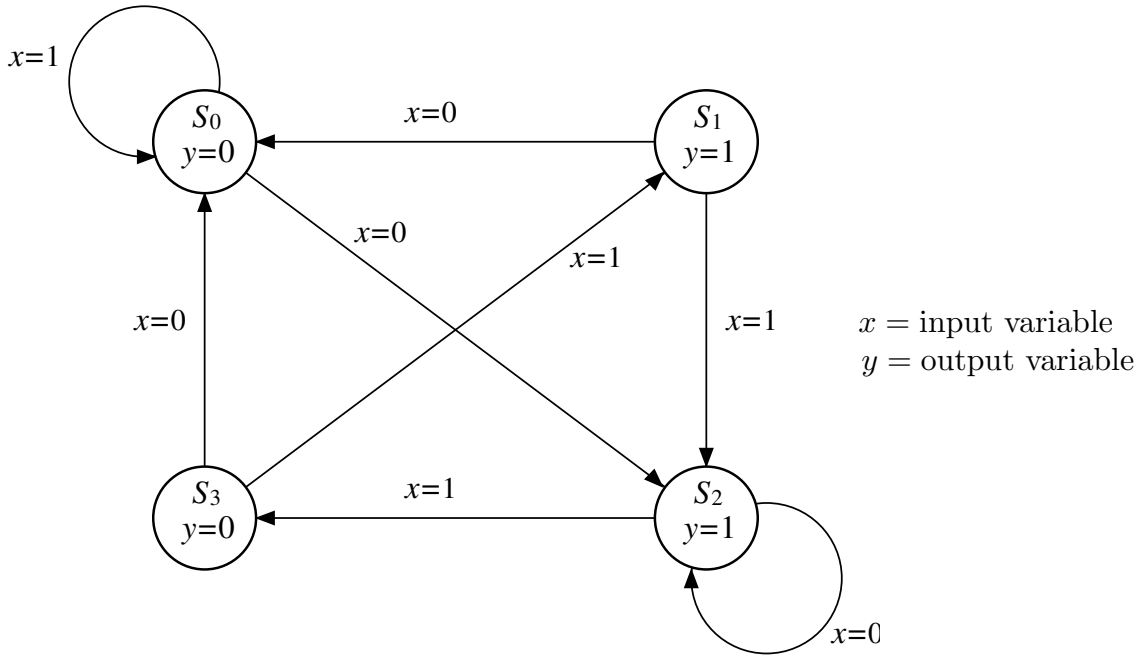
(i) NOR gates; [2 marks]

(ii) NAND gates. [2 marks]

Assume that complemented input variables are available.

2 Digital Electronics

Consider the following state diagram



and the state assignment $S_0 = 00$, $S_1 = 01$, $S_2 = 10$ and $S_3 = 11$.

(a) Write down the state table and derive the minimised Boolean expressions for implementing the next-state and output functions. Assume the use of D-type flip-flops for the state registers. Note that state $= (Q_1, Q_0)$. [10 marks]

(b) An alternative is to use a 1-hot state machine with the following state assignment: $S_0 = 0001$, $S_1 = 1000$, $S_2 = 0010$ and $S_3 = 0100$. Determine Boolean expressions for implementing the next-state and output functions assuming the use of D-type flip-flops. Note that state $= (Q_3, Q_2, Q_1, Q_0)$. [7 marks]

(c) What problem may arise with the approach proposed in part (b)? Briefly describe *two* solutions to this problem. [3 marks]

SECTION B

3 Discrete Mathematics I

(*a*) Given $a, b \in \mathbb{N}$ with $a \geq b$ prove carefully that there are unique values $q, r \in \mathbb{N}$ such that $a = qb + r$ and $0 \leq r < b$. [6 marks]

(*b*) Prove further that the highest common factor of a and b is equal to the highest common factor of b and r. [2 marks]

(*c*) Derive Euclid's algorithm for finding the highest common factor of two numbers. [3 marks]

(*d*) Determine the algorithm's efficiency by finding a limit for the number of divisions required in its execution expressed as a function of a. [3 marks]

(*e*) Find all values $x, y \in \mathbb{Z}$ satisfying $72x + 56y = 40$. [3 marks]

(*f*) Find all values $z \in \mathbb{Z}$ satisfying $56z \equiv 24 (\text{mod } 72)$. Express the answer in the form $z \equiv a (\text{mod } m)$. [3 marks]

4 Discrete Mathematics I

(*a*) State and prove the Chinese Remainder Theorem concerning the simultaneous solution of two congruences to co-prime moduli and the uniqueness of that solution. [8 marks]

(*b*) Consider an extension to solve a set of r simultaneous congruences:

$$\begin{aligned} x &\equiv a_1 (\text{mod } m_1) \\ x &\equiv a_2 (\text{mod } m_2) \\ &\vdots \\ x &\equiv a_r (\text{mod } m_r) \end{aligned}$$

where $i \neq j \Rightarrow (m_i, m_j) = 1$ and $M = m_1 m_2 \ldots m_r$.

(*i*) Prove that $(m_i, M/m_i) = 1$ for $1 \leq i \leq r$. [3 marks]

(*ii*) Explain briefly how to find s_i and t_i so that $m_i s_i + M t_i / m_i = 1$ for $1 \leq i \leq r$. It is not necessary to give a detailed algorithm. [2 marks]

(*iii*) Let $c = a_1 t_1 m_2 m_3 \ldots m_r + m_1 a_2 t_2 m_3 \ldots m_r + m_1 m_2 a_3 t_3 \ldots m_r + \cdots + m_1 m_2 m_3 \ldots a_r t_r$.
Show that $c \equiv a_i (\text{mod } m_i)$ for $1 \leq i \leq r$. [4 marks]

(*iv*) Show further that the solution is unique *modulo* M. [3 marks]

SECTION C

5 Discrete Mathematics II

The purpose of this question is to look at a method for counting certain finite sets that arise as quotients under an equivalence relation; and to apply the method to count the number of injections between two finite sets.

For a set A, let $\mathsf{Bij}(A)$ be the set of bijections from A to A. An *A-action* on a set X is defined to be a function $\star : X \times \mathsf{Bij}(A) \to X$, typically written in infix notation so that $x \star \sigma = \star(x, \sigma)$, such that $x \star \mathsf{id}_A = x$ and $(x \star \sigma) \star \tau = x \star (\sigma \circ \tau)$ for all $x \in X$ and $\sigma, \tau \in \mathsf{Bij}(A)$.

(*a*) Let $\star : X \times \mathsf{Bij}(A) \to X$ be an A-action on X. Show that the relation $\sim$ on X defined by $x \sim y \overset{\text{def}}{\iff} \exists\, \sigma \in \mathsf{Bij}(A).\ x = y \star \sigma$, for all $x, y \in X$, is an equivalence relation. [6 marks]

(*b*) As usual, let $[x]_\sim \overset{\text{def}}{=} \{\, y \in X \mid x \sim y \,\}$ be the equivalence class of $x \in X$ under the equivalence relation $\sim$. Furthermore, for $x \in X$, let $e_x : \mathsf{Bij}(A) \to [x]_\sim$ be the function defined by $e_x(\sigma) \overset{\text{def}}{=} x \star \sigma$, for all $\sigma \in \mathsf{Bij}(A)$.

For $x \in X$, prove that e_x is surjective. For A a finite set of size n, what does this tell us about the size of $[x]_\sim$, for $x \in X$? [2 marks]

(*c*) An A-action on X is said to be *faithful* if the function e_x is injective for all $x \in X$. In this case:

(*i*) If A is a finite set of size n, what is the size of each $[x]_\sim$, for $x \in X$?

(*ii*) If, in addition, X is a finite set of size m, what is the size of the set of equivalence classes $X/_\sim \overset{\text{def}}{=} \{\, [x]_\sim \mid x \in X \,\}$?

Justify your answers. [6 marks]

(*d*) For sets A and B, let $\mathsf{Inj}(A, B)$ be the set of injections from A to B. Show that the function $\bullet : \mathsf{Inj}(A, B) \times \mathsf{Bij}(A) \to \mathsf{Inj}(A, B)$ defined by $\iota \bullet \sigma \overset{\text{def}}{=} \iota \circ \sigma$, for all $\iota \in \mathsf{Inj}(A, B)$ and $\sigma \in \mathsf{Bij}(A)$, is an A-action on $\mathsf{Inj}(A, B)$. Prove also that it is faithful. [6 marks]

Note that since $\mathsf{Inj}(A, B)/_\sim \;\cong\; \{\, S \subseteq B \mid S \cong A \,\}$, it follows from the results in (*c*)(*ii*) and (*d*) that, for A and B finite, $\#\big(\mathsf{Inj}(A, B)\big) = \binom{\#B}{\#A}(\#A)!$.

6 Discrete Mathematics II

(a) Let V be a set of propositional variables, and let $\mathcal{F}_V$ be the set of propositional formulae (or Boolean propositions) with propositional variables in V.

Consider the set of rule instances R given by

$$\boxed{\text{Axiom K}} \quad \frac{}{A \Rightarrow (B \Rightarrow A)}$$

$$\boxed{\text{Axiom S}} \quad \frac{}{\big(A \Rightarrow (B \Rightarrow C)\big) \Rightarrow \big((A \Rightarrow B) \Rightarrow (A \Rightarrow C)\big)}$$

$$\boxed{\text{Axiom C}} \quad \frac{}{(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)} \qquad \boxed{\text{Rule MP}} \quad \frac{A \qquad A \Rightarrow B}{B}$$

where $A, B, C \in \mathcal{F}_V$.

As usual, let $\mathcal{I}_R \subseteq \mathcal{F}_V$ denote the set inductively defined by R (that is, the smallest R-closed set). Furthermore, let $\mathcal{T} \subseteq \mathcal{F}_V$ be the set of tautologies.

You are required to establish that $\mathcal{I}_R \subseteq \mathcal{T}$, by rule induction. Specifically, state precisely what needs to be proved with respect to each of the Axioms K, S, C and the Rule MP; but only give details of the proofs associated to Axiom C and Rule MP. [12 marks]

[One can also show that $\mathcal{T} \subseteq \mathcal{I}_R$; but this is outside the scope of the question.]

(b) The purpose of this part of the question is to study diagonalisation, or Cantor's diagonal argument, and one of its consequences.

For sets X and Y, let $(X \to Y)$ denote the set of all functions from X to Y.

(i) A function $f : X \to X$ is said to have a fixed point if there exists an element $x \in X$ such that $f(x) = x$; an element with this property is called a *fixed point* of the function.

Prove the following *Diagonalisation Theorem*: For sets N and X, if there exists a surjection $N \twoheadrightarrow (N \to X)$ then every function $X \to X$ has a fixed point. [4 marks]

[Hint: Let $e : N \twoheadrightarrow (N \to X)$ be a surjection and, for $f : X \to X$, consider the function $\varphi : N \to X$ defined by $\varphi(n) \stackrel{\text{def}}{=} f\big(e(n)(n)\big)$, for all $n \in N$.]

(ii) Using the Diagonalisation Theorem, or otherwise, show that if there exists a surjection $D \twoheadrightarrow (D \to D)$, for a set D, then D has exactly one element. [4 marks]

SECTION D

7 Software Design

Consider the design of an appointment reminder service using Web and SMS technologies. Describe, using text and/or diagrams where appropriate, the following aspects of the design:

(a) *two* use cases; [4 marks]

(b) *three* classes; [3 marks]

(c) a sequence of interaction between classes; [3 marks]

(d) the possible states of an instance of the reminder class; [3 marks]

(e) *three* named variables, with their rôles, in a routine that scans for the next due reminder; [1 mark each]

(f) one precondition *and* one postcondition, for a routine that adds new reminders. [2 marks each]

8 Regular Languages and Finite Automata

(a) State the *Pumping Lemma* for regular languages. Is every language that satisfies the pumping lemma property a regular language? [5 marks]

(b) State, with justification, whether or not each of the following languages is regular. Any standard results you use should be clearly stated, but need not be proved.

(i) $L_1 = \{ww \mid w \in \{a\}^*\}$ [3 marks]

(ii) $L_2 = \{ww \mid w \in \{a, b\}^*\}$ [3 marks]

(iii) $L_3 = \{w_1 w_2 \mid w_1 \in \{a\}^* \text{ and } w_2 \in \{b\}^*\}$ [3 marks]

(iv) $L_4 = \{w \mid w \in \{a, b\}^*$ and w contains the same number of as and bs$\}$ [3 marks]

(v) $L_5 = \{w \mid w \in \{a, b\}^*$, w contains the same number of as and bs, and that number is no more than 128$\}$ [3 marks]

9 Professional Practice and Ethics

(*a*) The U.K. Disability Discrimination Act 1995 places a duty on organisations to provide equality of access for disabled people. Web-based content can fall under the provisions of the Act wherever it is used to provide goods, services, staff information (such as on an intranet) or education. Name *two* kinds of disability which may limit Web access. How can Web access be improved for people with those kinds of disability? [4 marks]

(*b*) Present *two* credible moral justifications someone gaining illegal access to a computer might give for this activity. What arguments would you present against those reasons? [4 marks]

(*c*) Part 5 of The Police and Justice Bill 2006 introduces amendments to the Computer Misuse Act (CMA) of 1990. One of the amendments increased the scope of the law to include denial of service attacks. How was this done? A further clause, 3A, was added to the CMA 1990. What acts were criminalised by this clause, and what objections have been raised against the clause? [4 marks]

(*d*) "Honest, upright, law-abiding citizens have nothing to fear from the distribution of their personal data." Do you agree or not? Give at least *three* reasons for your position and *one* reasonable objection to it. [4 marks]

(*e*) What is the consequentialist justification for laws that give ownership and control of software to individuals or corporations (proprietary software)? What is the basic dilemma in giving individuals the ownership and control of software they wrote? Is there any alternative to working with privately-owned (proprietary) software? [4 marks]

END OF PAPER