COMPUTER SCIENCE TRIPOS Part IA

Tuesday 6 June 2006 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

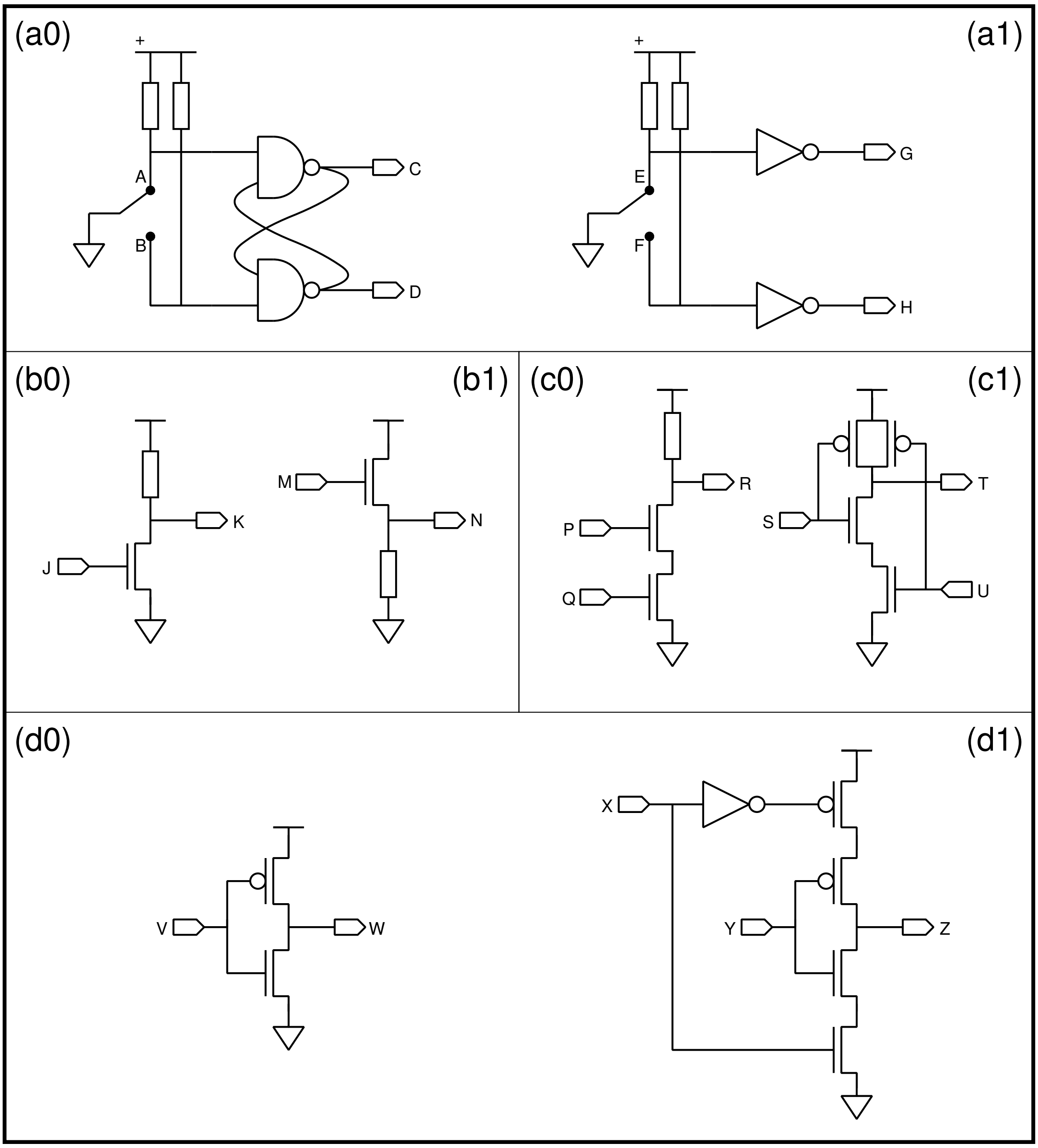
STATIONERY REQUIREMENTS
Script Paper
Blue Coversheets
Tags

SECTION A

1 Digital Electronics

Four pairs of circuits (a0, a1), (b0, b1), (c0, c1) and (d0, d1) are presented below. What is the operation of each circuit and how does it compare with its pair?

[5 marks each]



2 Digital Electronics

(*a*) An electronic die may be constructed from seven LEDs laid out in the pattern below. The LEDs are to be driven by signals (a,b,c,d).

a c

b d b

c a

A binary-to-die decoder is described in the left-hand table below with inputs (n2,n1,n0) and outputs (a,b,c,d). X represents *don't care*.

(*i*) What are the minimum sum-of-product equations mapping the inputs to the outputs? [4 marks]

(*ii*) If the inputs to the decoder were to be driven by a three D flip-flop state machine, what are the minimum sum-of-products equations for the next state functions for (n2,n1,n0) to count continuously $1, 2, 3, 4, 5, 6, 1, \ldots$? [6 marks]

(*b*) An alternative implementation is to use a 1-hot state machine plus a different decoder to form a rolling die (see right-hand table below). The states are (h1,h2,h3,h4,h5,h6) and the die output this time is (A,B,C,D).

(*i*) What is the minimal free running 1-hot state machine constructed from D flip-flops? You may assume that the D flip-flops have preset and clear inputs. [3 marks]

(*ii*) What are the minimum sum-of-product equations for mapping the 1-hot states to die outputs? [4 marks]

(*iii*) Is the first implementation in part (*a*) quicker or slower than the one in part (*b*)? [3 marks]

binary to die decoder

input			output			
n2	n1	n0	a	b	c	d
0	0	0	X	X	X	X
0	0	1	0	0	0	1
0	1	0	1	0	0	0
0	1	1	1	0	0	1
1	0	0	1	0	1	0
1	0	1	1	0	1	1
1	1	0	1	1	1	0
1	1	1	X	X	X	X

1-hot to die decoder

input						output			
h6	h5	h4	h3	h2	h1	A	B	C	D
0	0	0	0	0	1	0	0	0	1
0	0	0	0	1	0	1	0	0	0
0	0	0	1	0	0	1	0	0	1
0	0	1	0	0	0	1	0	1	0
0	1	0	0	0	0	1	0	1	1
1	0	0	0	0	0	1	1	1	0

SECTION B

3 Discrete Mathematics I

(*a*) State the Fermat–Euler theorem, carefully defining any terms that you use. Deduce that $2^p \equiv 2 \pmod{p}$ for any prime p. [5 marks]

(*b*) Explain how this result can be used to show that a number is composite without actually finding a factor. Give an example. [3 marks]

(*c*) Let $M_m = 2^m - 1$ be the m^{th} Mersenne number. Suppose that m is composite. Prove that M_m is composite. [3 marks]

(*d*) A composite number m that satisfies $2^m \equiv 2 \pmod{m}$ is known as a *pseudo-prime*.

(*i*) Suppose that m is prime. Prove that M_m is either prime or a pseudo-prime. [3 marks]

(*ii*) Suppose that m is a pseudo-prime. Prove that M_m is a pseudo-prime. [3 marks]

(*iii*) Deduce that there are infinitely many pseudo-primes. [3 marks]

4 Discrete Mathematics I

Consider two natural numbers a, $b \in \mathbb{N}$.

(a) Define the highest common factor (a, b) of a and b. [2 marks]

(b) Show that the set of linear combinations of a and b is equal to the set of multiples of their highest common factor:
$\{as + bt \mid s, t \in \mathbb{Z}\} = \{v\,(a, b) \mid v \in \mathbb{Z}\}$ [8 marks]

Suppose that a and b are co-prime, so $(a, b) = 1$. Define a *natural linear combination* of $a, b \in \mathbb{N}$ to be $as + bt$ with $s, t \in \mathbb{N}_0$.

(c) Show that $ab - a - b$ cannot be expressed as a natural linear combination of a and b. [2 marks]

(d) Show that any natural number greater than $ab - a - b$ can be expressed as a natural linear combination of a and b. [6 marks]

[Hint: recall the complementary function for a linear Diophantine equation.]

(e) Royal Mail first class stamps cost 32p each and second class stamps cost 23p each. What is the largest postage that cannot be paid exactly with first and second class stamps? [2 marks]

SECTION C

5 Discrete Mathematics II

(a) What does it mean for a function to be an *injection*, *surjection* and *bijection*? [3 marks]

(b) Let $I = \{x \in \mathbb{R} \mid x > 1\}$. Define a binary relation $g \subseteq I \times I$ by taking

$$(u, v) \in g \;\text{ iff }\; \frac{1}{u} + \frac{1}{v} = 1 \;.$$

(i) Express v as a formula in u for $(u, v) \in g$. Deduce that g is a function $g : I \to I$. [2 marks]

(ii) State what properties are required of a function $h : I \to I$ in order for h to be an inverse function to g. Define an inverse function to g and prove that it has the desired properties. Deduce that $g : I \to I$ is a bijection. [6 marks]

(c) (i) Let X be a set. Prove there is no injection $f : \mathcal{P}(X) \to X$.
[Hint: consider the set $Y \stackrel{\text{def}}{=} \{f(Z) \mid Z \subseteq X \;\wedge f(Z) \notin Z\}$.] [5 marks]

(ii) Suppose now that the set X has at least two distinct elements. Define an injection $k : \mathcal{P}(X) \to (X \to X)$, from the powerset of X to the set of functions from X to X. [2 marks]

(iii) Prove that there is no injection from $(X \to X)$ to X when the set X has at least two distinct elements. [You may assume that the composition of injections is an injection.] [2 marks]

6 Discrete Mathematics II

(*a*) (*i*) Draw the truth tables to illustrate the truth values of $\mathtt{A} \Rightarrow \mathtt{B}$ and $\mathtt{A} \Leftrightarrow \mathtt{B}$ in terms of the truth values of $\mathtt{A}$ and $\mathtt{B}$. [2 marks]

(*ii*) By considering their truth tables, establish the following equivalences of boolean propositions:

1. $\mathtt{A} \Leftrightarrow (\mathtt{B} \Leftrightarrow \mathtt{C}) = (\mathtt{A} \Leftrightarrow \mathtt{B}) \Leftrightarrow \mathtt{C}$. [5 marks]

2. $(\mathtt{F} \Leftrightarrow \mathtt{B}) = \neg\mathtt{B}$, where $\mathtt{F}$ is the proposition "false". [2 marks]

3. $\neg(\mathtt{B} \Leftrightarrow \mathtt{C}) = ((\neg\mathtt{B}) \Leftrightarrow \mathtt{C})$. [2 marks]

(*iii*) By assigning suitable truth values to propositions $\mathtt{B}$ and $\mathtt{C}$, explain why the equivalence 3 above fails to hold if "$\Leftrightarrow$" is replaced by "$\Rightarrow$". [3 marks]

(*b*) The set S is defined to be the least subset of (positive) natural numbers $\mathbb{N}$ such that:

$1 \in S$;

if $n \in S$, then $3n \in S$;

if $n \in S$ and $n > 2$, then $(n - 2) \in S$.

Show that $S = \{m \in \mathbb{N} \mid \exists r, s \in \mathbb{N} \cup \{0\}.\ m = 3^r - 2s\}$. [6 marks]

SECTION D

7 Software Design

The William Gates Building has a centrally managed security system, dividing the building into zones to which different classes of user can gain access. All building users are issued with security cards that let them pass through doors into permitted zones.

(*a*) Imagine you are designing the security system from scratch. Draw *two* diagrams suitable for discussing the operation of the system with

(*i*) future building users;

(*ii*) client engineering staff who will approve and manage the data model. [4 marks each]

(*b*) Outline a project plan suitable for the management of this project, including a brief explanation of the kind of activity to be carried out in each phase. [6 marks]

(*c*) The glass front doors to the building, originally conventional manual swing doors that required card access outside working hours, were inappropriate for wheelchair access. It was decided to replace them with automatic doors that slide open as you approach.

Draw *two* statechart diagrams showing the behaviour of the doors

(*i*) before this change;

(*ii*) after this change, when the door operation state must be combined with the operation of the access-control system. [2 marks each]

(*d*) If the software to control the sliding doors were to be implemented as an additional component of the security system, what earlier design precautions might have made such a change more straightforward? [2 marks]

8 Regular Languages and Finite Automata

(*a*) Suppose that L_1 and L_2 are regular languages (over the same alphabet Σ) accepted by deterministic finite automata M_1 and M_2 respectively. Show that there is a *deterministic* finite automaton M such that for all strings u over Σ, M accepts u if and only if $u \notin L_1$ or $u \in L_2$. [8 marks]

(*b*) Show that if a deterministic finite automaton M over alphabet Σ accepts all strings of length less than the number of states in M, then it must accept all strings over Σ. [4 marks]

(*c*) What does it mean for two regular expressions over an alphabet Σ to be *equivalent*? Using parts (*a*) and (*b*), or otherwise, describe an algorithm for deciding equivalence of regular expressions. State carefully any standard results that you rely upon. [8 marks]

9 Professional Practice and Ethics

(*a*) Name *two* kinds of ethical theory and give a defining characteristic for each. [4 marks]

(*b*) The Code of Conduct of the British Computer Society has 17 clauses. The clauses are organised under four main headings: The Public Interest, Duty to Relevant Authority, Duty to the Profession, and Professional Competence and Integrity. State *one* of the requirements under *each* heading. [4 marks]

(*c*) The *Computer Misuse Act 1990* created three new offences. Name *two* of them. Apart from the person who actually commits the offence, to whom else does the law extend? [4 marks]

(*d*) The *Data Protection Act 1998* sets out eight principles for the protection of privacy in data collection, handling and distribution. Name *two* of these principles and explain how each serves to protect privacy. [4 marks]

(*e*) Three different kinds of law have been used to establish ownership and control of software and each has some problems. Name *two* kinds of such law and state at least *one* unique characteristic or problem associated with each kind. [4 marks]

END OF PAPER