# DUDEBASE COLLEGES PROGRESS EXAMINATION

Tuesday 18 January 2022 10:15 – 11:15

Computer Science Paper 2 (CST IA)

*Answer* **one** *question from each Section. Each question is worth the same number of marks.*

*Write on* **one** *side of the paper only.*

*Write your name and the question number at the top of every sheet, and tie your answers into separate bundles (one for each question).*

**DO NOT TURN OVER THE QUESTION PAPER UNTIL TOLD BY THE INVIGILATOR THAT YOU MAY DO SO**

## SECTION A

### 1 Digital Electronics

An *M-N Flip Flop* has the following truth table.

| $M$ | $N$ | $Q'$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | $Q$ |
| 1 | 1 | $\bar{Q}$ |

($a$) If the current output, $Q$, is 1 and on the next clock edge we want it to become 0, which two pairs of control signals $M, N$ could be used? [2 marks]

($b$) Hence or otherwise determine the excitation table for an $M$-$N$ Flip Flop using notation of the form *00 or 11* where useful. [3 marks]

($c$) A divide-by-7 counter, built with $M$-$N$ Flip Flops, is required.

($i$) Is a Moore Machine or a Mealy Machine appropriate? [1 mark]

($ii$) Determine the state transition table. [2 marks]

($iii$) Add next state controls to your state transition table. [4 marks]

($iv$) Using Karnaugh Maps, identify the combinatorial circuits that compute the next state control signals that will allow the counter to run at the greatest possible frequency. [4 marks]

($v$) Draw a circuit diagram for the divide-by-7 counter. Label the most and least significant bits of the output. [2 marks]

($vi$) Is your circuit self-starting? [2 marks]

## 2 Digital Electronics

($a$) Consider the following transition table for a state machine with two inputs and one output:

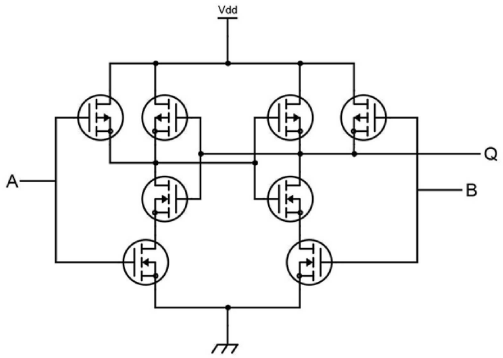
| Current state, S | Output, Q | Next state, $S^0$ | | | |
|---|---|---|---|---|---|
| | | X = 0 Y = 0 | X = 0 Y = 1 | X = 1 Y = 0 | X = 1 Y = 1 |
| A | 0 | A | A | B | B |
| B | 1 | A | A | C | D |
| C | 1 | A | A | C | D |
| D | 0 | D | D | E | E |
| E | 1 | D | D | F | A |
| F | 1 | D | D | F | A |

($i$) Does this table describe a Mealy Machine or a Moore Machine? [1 mark]

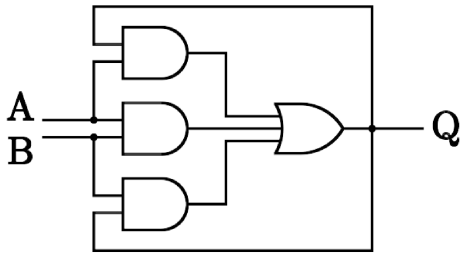
($ii$) Fully simplify the state machine. [4 marks]

($b$) Deduce the details and operation of the following circuits. [3 marks each]

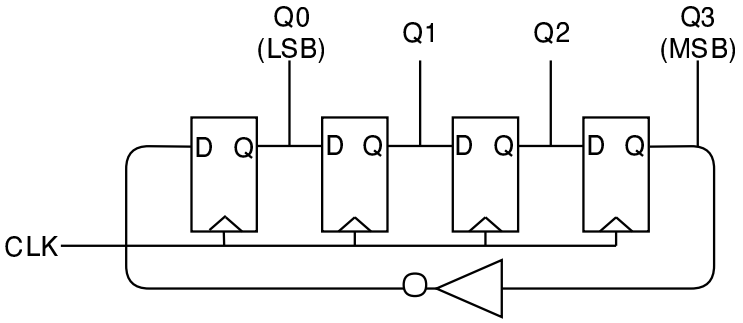
($i$)




($ii$)




($iii$) (initially all $Q_i = 0$)




($c$) Derive combinatorial expressions to convert the output from c(iii) into the natural binary count 000, 001, 010, ... 111, 000, ... [4 marks]

($d$) What would be the advantages/disadvantages of using the circuit in c(iii) to drive a finite state machine, compared to using a 3-bit synchronous counter designed such that its outputs are 000, 001, 010, ..., 111, 000? [2 marks]

## SECTION B

### 3 Discrete Mathematics

Consider positive integers $m$ and $n$ such that

$$\left(n^2 - mn - m^2\right)^2 = 1$$

($a$) What is the value of $\gcd(m, n)$? [4 marks]

($b$) Show that $n \geq m$. [4 marks]

($c$) Show that if $n \neq m$, $(m, n)$ satisfies the initial equation if and only if $(n-m, m)$ also satisfies the equation. [2 marks]

($d$) If both $m$ and $n$ are positive integers between 1 and 2016 and satisfy the initial equation, what is the maximal value of $m + n$? [10 marks]

## 4 Discrete Mathematics

(*a*) For $x, y \in \mathbb{Z}, k \in \mathbb{N}, m \in \mathbb{N}, m > 0$, prove:

$$x \equiv y \pmod{m} \Rightarrow x^k \equiv y^k \pmod{m}$$

[4 marks]

(*b*) Recall that the Diffie-Hellman key exchange protocol allows two parties, Alice and Bob, to establish a shared secret $\left[g^{ab}\right]_p$ over a public channel, where prime $p$ and $g \in \mathbb{Z}_p$ are pre-arranged parameters, and $a, b \in \mathbb{Z}_p$ are random numbers picked by Alice and Bob respectively.

(*i*) Outline the calculations performed and messages sent by Alice and Bob to establish the shared secret. [3 marks]

(*ii*) Using part (a) or otherwise, justify that Alice and Bob do in fact receive the same shared secret. [3 marks]

(*iii*) Using $p = 79, g = 39, a = 20$, calculate the number sent from Alice to Bob. [3 marks]

(*iv*) You overhear the messages 57 and 54 sent between Alice and Bob during the exchange using $p = 71, g = 25$. These parameters are poorly chosen since $25^5 \equiv 1 \pmod{71}$. Find the shared secret. [3 marks]

(*v*) Determine all possibilities for the values of $a$ and $b$ that were picked by Alice and Bob in part (iv). [2 marks]

(*vi*) In light of the problem revealed by part (iv), for $p = 11$ would you suggest Alice and Bob use $g = 5$, or $g = 7$? [2 marks]

**END OF PAPER**