



Galway-Mayo Institute of Technology
Semester 2 Examinations 2017/2018

MODULE: COMP08015 – Theory of Algorithms

PROGRAMME(S):

GA_KSOFG_H08 B.Sc. (Honours) Software Development

YEAR(S) OF STUDY: 4

EXAMINERS:

Dr. Ian McLoughlin (Internal)

Dr. Des Chambers (External)

Mr. Tom Davis (External)

TIME ALLOWED: 2 hours

INSTRUCTIONS: Answer 3 questions. All questions carry equal marks.

Please do not turn this page until you are instructed to do so.

The use of programmable or text storing calculators is expressly forbidden. Please note that where a candidate answers more than the required number of questions, the examiner will mark all questions attempted and then select the highest scoring ones.

There are no additional requirements for this paper.

Question 1 (100 total marks)

Use the input alphabet $\{0, 1\}$ in answering the following question about Turing machines.

- (a) Explain in your own words what a Turing machine is. (40 marks)
- (b) Give the state table for a Turing machine that accepts all strings that are of even length and contain an even number of 1's. (Assume zero is an even number.) (40 marks)
- (c) Give the state table for a Turing machine that accepts only the empty string. (20 marks)

Question 2 (100 total marks)

Consider the language $L = \{0^i 1^i \mid i \in \mathbb{N}, i > 0\}$ over the alphabet $A = \{0, 1\}$.

- (a) List the five shortest strings in L , and give a general formula for the length of strings in L in terms of i . (40 marks)
- (b) Explain what is meant by A^* (where $*$ is the Kleene star) and list the six shortest strings that are in A^* but not in L . (40 marks)
- (c) State whether A^* and L^* are equivalent and explain your reasoning. (20 marks)

Question 3 (100 total marks)

Consider the following Racket code and answer the questions below.

```
1  (define (cont l a)
2    (if (null? l) #f
3        (if (= (car l) a) #t
4            (cont (cdr l) a))))
5
6  (define (niq l)
7    (if (null? l) null
8        (if (cont (cdr l) (car l)) (niq (cdr l))
9            (cons (car l) (niq (cdr l)))))))
10
11 (niq (list 1 2 2 3))
```

- (a) Explain what each of the three Racket procedures `car`, `cdr`, and `cons` do, and explain the difference between `null` and `null?` as used above. (40 marks)
- (b) Determine what the output of the last line of the code is. Show your workings. (40 marks)
- (c) Functional programming languages are said to avoid side-effects. Give an example of a side effect in Java. (20 marks)

Question 4 (100 total marks)

This question is about the SHA-256 and MD5 hashing standards.

- (a) Explain how and why passwords on a modern Linux system are stored as hashed values. (40 marks)
- (b) It has been suggested that SHA-256 is preferable to MD5 when calculating password hashes because MD5 is known to be vulnerable to known collision attacks. Explain what a collision attack is and why it matters if MD5 is vulnerable. (40 marks)
- (c) Cryptographic hash functions are sometimes called one-way functions. Explain what a one-way function is and suggest whether SHA-256 is such a function. (20 marks)