Ollscoil na hÉireann
The National University of Ireland

Coláiste na hOllscoile, Corcaigh
University College, Cork

End-Semester Examination
Semester 1 - Winter 2018

CS6320 Formal Methods for Distributed Systems
2018-2019

M.Sc. Computer Science

Dr. Lucy Hederman
Prof. Cormac Sreenan
Dr. John Herbert

Answer all questions

Total marks: 40

Time: 60 minutes

Minutes per mark: 1.2

(a) State precisely the meaning of the triple {P}C{Q} as used in Floyd-Hoare logic for program verification. (3 marks)

(b) In the context of software program verification describe the general method using Floyd-Hoare logic of relating a specification of requirements to a **complete** program implementing the requirements. (5 marks)

(c) Give a brief description of the successful use of formal methods within a large technology company (such as Intel or Microsoft or Amazon). (3 marks)

(d) State two important difficulties of using formal methods in industry. (2 marks)

(e) Give a brief overview of the technique of "model checking" as used in formal verification of systems. (3 marks)

(f) State why Ordered Binary Decision Diagrams (OBDDs) are important for model-checking tools such as SMV. (2 marks)

(g) State what is similar and also state two differences between Meyer's Design by Contract and the Floyd-Hoare logic. (3 marks)

A class represents a simple lift controller. This class has boolean attributes representing the state of the lift: out_of_order; door_is_open; moving_up; moving_down; and stopped.

(h) Following Meyer's Design by Contract approach, write down an invariant for this class in standard mathematical logic stating the most important invariant properties. (2 marks)

(i) The class includes two operations (methods): GoUp() making the lift go up; OpenDoor() opening the lift doors. Specify these two operations using contracts expressed in standard mathematical logic. (2 marks)

An algorithm enforcing mutual exclusion between two processes, pr1 and pr2, is described by the following SMV outline program where n, t, and c correspond to a process being in non-critical, trying and critical states.

```
MODULE main
    VAR
        pr1 : process prc(pr2.st, turn, 0);
        pr2 : process prc(pr1.st, turn, 1);
        turn : boolean;
    ASSIGN
        init(turn) := 0;

A

MODULE prc(other-st, turn, myturn)
    VAR
        st : {n, t, c};
    ASSIGN
        init(st) := n;

        next(st) :=
            case
B
            esac;

        next(turn) :=
            case
C
            esac;

D
```

(j) For position **A**, write down the SPEC in CTL (Computational Tree Logic) for one safety and one liveness requirement property of the algorithm**.** (2 marks)

(k) For position **B**, write down the missing lines of code. (4 marks)

(l) For position **C**, write down the missing lines of code. (2 marks)

(m) State precisely what a FAIRNESS condition means, and explain how it helps in model checking. (3 marks)

(n) For position D write down two FAIRNESS conditions for this protocol. (2 marks)

(o) Explain why asynchronous models are often required when modeling a distributed system in the SMV tool. (2 marks)