Ollscoil na hÉireann
The National University of Ireland

Coláiste na hOllscoile, Corcaigh
University College, Cork

Mid-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: 50 minutes

Minutes per mark: 1.25

(a) State two important advantages and one important limitation of using formal methods (based on mathematical logic) as part of a software development process. (3 marks)

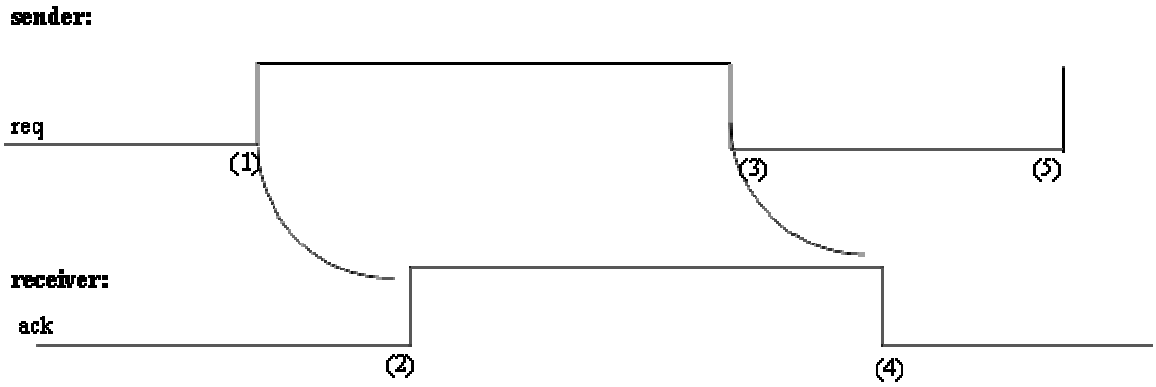
(b) Give examples from a standard logic to illustrate what is meant by the syntax, semantics and rules of inference of a mathematical logic. (3 marks)

(c) Explain, in your own words, what is meant by the soundness and completeness of a logical system? (2 marks)

(d) Discuss briefly whether most logical systems have both soundness and completeness? (2 marks)

(e) The BAN (Burrows Abadi Needham) logic for authentication is an example of an axiomatized logic. State what is meant by an axiomatized logic. (2 marks)

(f) State one advantage and one limitation of axiomatized logics. (2 marks)



Property A: $\Box$ $req \ IMP \ (\Diamond \ ack)$

Property B: $\Box$ $(\text{NEG} \ ack) \ IMP \ (\text{NEG} \ ack \ U \ req)$

The following questions are based on the above timing diagram of the four-phase handshaking protocol, and the given properties.

(g) State clearly the meaning of Property A in your own words. (2 marks)

(h) State clearly the meaning of Property B in your own words. (2 marks)

(i) State which part of the timing diagram Property A relates and which part Property B relates to (e.g. 2 to 3). (2 marks)

(j) A computer system controls a bridge carrying a road across a river, and provides a service for boats using the river and vehicles on the road. The computer system raises and lowers the bridge, and controls traffic lights at the ends of the bridge. A boat request button indicates that a boat needs the bridge to be raised, and a boat cleared sensor indicates that a boat has passed and the bridge can be lowered. Draw an abstract view of the computer system, showing the system boundary, the interface signals, and internal states if needed.
State precisely in natural language four important requirements of this control system.
Indicate with a label one safety and one liveness property among these four.
Express these four requirement properties also in mathematical logic.

(10 marks)

$$\vdash_{def} \; SWITCH(cont,in1,in2,out) =$$
$$\exists\ p1\ p2\ p3.$$
$$INV(cont,p1) \wedge$$
$$AND(in1,cont,p2) \wedge$$
$$AND(in2,p1,p3) \wedge$$
$$OR(p2,p3,out)$$

(k) The above term is a definition. What do we mean by a definition, and why is a definition logically important? (2 marks)

(l) Explain in detail what the different parts of the term on the right hand side of the equation are meant to represent, and explain what the overall right hand side represents. (3 marks)

The specification of requirements for the above system (SWITCH) is given by

$\vdash_{def}$ SWITCH_SPEC(cont, in1, in2, out) = (out = IF cont THEN in1 ELSE in2)

(m) State, in mathematical logic, a statement of correctness relating the implementation to the specification. (1 mark)

(n) Outline the general steps in doing the formal verification (proof of correctness) of the structural implementation, described by SWITCH, with respect to the specification of requirements, SWITCH_SPEC. (4 marks)