UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2002

MSci Honours Degree in Mathematics and Computer Science Part IV
MEng Honours Degrees in Computing Part IV
MSc in Advanced Computing
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant examinations for the
Associateship of the City and Guilds of London Institute
This paper is also taken for the relevant examinations for the
Associateship of the Royal College of Science

PAPER C481

MODELS OF CONCURRENT COMPUTATION

Thursday 2 May 2002, 10:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators not required

1a Show that the following laws are equivalent in CCS:

$$P+\tau.P = \tau.P$$
$$P+\tau.(P+Q) = \tau.(P+Q)$$

State any laws you use.

b i) Define *weak bisimulation* and *weak equivalence* $\approx$.

ii) Show that $\approx$ is transitive.

c Show that $P \approx Q$, where

$$P =_{df} a.(\tau.b+\tau) + a.b.\tau$$
$$Q =_{df} a.(\tau.b+\tau)$$

d Show that $P \approx Q$, where

$$P =_{df} a.P + \tau.a.P$$
$$Q =_{df} a.a.Q$$

State a simpler process R which is weakly equivalent to both P and Q.

The four parts carry, respectively, 20%, 35%, 20%, 25% of the marks.

2a State the definition of the *satisfaction relation* $\models$ for weak (i.e. with τ actions hidden) Hennessy-Milner logic.

b Show that $P \neq Q$, where

$$P =_{df} a.(b+c) + a.c + a.(b+\tau.c)$$
$$Q =_{df} a.(b+c) + a.c$$

State any theorem you use.

c State the definition of the *idling* transition relation in Temporal CCS (TCCS).

d An arcade game works as follows. When a coin is put in the slot, the player receives 100 units of playing time. At each unit of time the player can press the display or do nothing. If the player does not press for 5 units, the game goes into sleep mode, during which no playing time is used up. The game is reactivated by again pressing the display.

Model the game in TCCS. Explain your answer.

The four parts carry, respectively, 15%, 30%, 25%, 30% of the marks.

3a The following relates to the Spi calculus:

i) Define strong barb $P{\downarrow}n$

ii) Define weak barb $P{\Downarrow}n$

iii) Define testing equivalence $\simeq$

iv) Describe informally the properties of *authenticity* and *secrecy* as applied to an instance of a protocol in which A sends a message M to B.

b Two processes A and B and a server S are connected by public channels c_{AS} from A to S, c_{SB} from S to B, and c_{BA} from B to A. A and S share the key K_{AS}, and S and B share the key K_{SB}.

In a protocol, A sends a new key K_{BA} to B via S (using K_{AS} and K_{SB}) and then B sends message M to A using K_{BA}.

i) Write down the protocol as a sequence of messages.

ii) Formulate the protocol in the Spi calculus.

iii) Give a formal statement of the secrecy and authenticity properties for the protocol.

c A pay-per-view satellite broadcasting system works as follows: The company sends a new key K to the satellite on channel `newkey`. The satellite then broadcasts a programme on the public channel `broadcast` encrypted with K. The customer has a set-top box. When the customer puts a coin into a slot in the box, the box creates a unique session id and contacts the company on channel `subscribe` giving the id. The company returns K to the box. Finally the box receives the broadcast and emits it in plain text on channel `plain`.

Model the system consisting of `Satellite`, `Company`, and `Box` in the Spi calculus. Your `Company` and `Satellite` processes should be able to cope with any number of customers. Give a diagram showing processes and channel names.

The three parts carry, respectively, 35%, 40%, 25% of the marks.

4a Define the following as applied to Petri nets:

i) concurrent enabling

ii) live

iii) deterministic

iv) safe

b Two processes P_1,P_2 alternately start up (events a_1,a_2) and close down (events b_1,b_2). Thus a_1 alternates with b_1, and a_2 with b_2. In addition the start actions are required to alternate and the close actions also alternate. Thus a_1 alternates with a_2, and b_1 with b_2. Initially both processes are ready to start up, with P_1 being the first to start.

i) Model the system as a Petri net.

ii) Give a transition diagram for your net, complete with markings.

iii) Answer the following, giving brief explanations:

(1) Is the net live?

(2) Is the net deterministic?

(3) Is the net safe?

(4) Are all markings reachable?

iv) Model the system as an event structure, up to and including the second occurrence of each event.

The two parts carry, respectively, 25%, 75% of the marks.