CSE4213 Sample Examination
2002
Instructions to Candidates

1. Examination time 2 hours
2. Answer all questions
3. There are 10 questions
4. Each question is worth 8 marks
5. Total marks 80
6. Calculators are not allowed
7. Use left hand page for rough working; this page will NOT be marked unless explicitly requested.
8. The *Concise Summary of the B mathematical toolkit* is supplied.

1. B has been used to design the signalling and control systems for driverless trains on the Paris Metro system. Explain why.

(8 marks)

2. Explain the use of non-determinism in B specifications. Give an example to illustrate your answer.

(8 marks)

3. The INCLUDES, PROMOTES and EXTENDS clause in a B machine specification allow more complex specifications to be built from simple ones.

   - The INCLUDES clause names machine whose operations are available for use in the including machine, **but** these operations are not part of the including machine's operations.
   - The EXTENDS clause names machines whose operations are available for use in the including machine, **and** these operations are also part of the including machine's operations.
   - The PROMOTES clause names operations of an included machine that are also made available as pert of the including machines operations.

   Motivate the distinctions between these clauses from a software engineering perspective.
   (8 marks)

4. Give the Predicate Transformations of the following expressions:

   (a) $[skip]\ x > y$

   (b) $[x := a]\ \forall\, p.f(x) = p$

   (c) $[x := y || y := x]\ x > y$

   (d) $[x \in \{2, 4, 6\} \Rightarrow x := x/2]\ 2 \times x$

(8 marks)

5. The following B machine specification fragment is taken from DEMO2, which deals with a simple Lift system. Given that

   mov is the set of LIFTS in motion;

   dir is a total function of LIFTS to DIRECTIONS ($\{up, dn\}$), and describes in which direction a particular lift is travelling;

   flr is a total function of LIFTS to FLOORS ($bottomflr..topflr$), and describes which floor each lift is at;

   out is a relation from LIFTS to FLOORS, and describes which buttons inside the lifts have been pressed; and

   in is a relation from FLOORS to DIRECTIONS, and describes which buttons outside the lifts have been pressed:

   explain the first four (4) preconditions of the operation **Continue_Up** in English.

Continue_Up (ll) $\widehat{=}$
PRE
$ll \in mov \wedge$
$dir\ (\ ll\ ) = up \wedge$
$flr\ (\ ll\ ) < topfloor \wedge$
$ll \mapsto flr\ (\ ll\ ) \notin out \wedge$
$flr\ (\ ll\ ) \mapsto up \notin in \wedge$
$attr\_up\ (\ ll\ )$
THEN
$flr\ (\ ll\ ) := flr\ (\ ll\ ) + 1$
END ;

(8 marks)

6. In a railway system, trains are made up by joining a number of carriages together, and numbered from the front of the train. At the front of the train is a locomotive, required to haul the train.

   In specifying a train despatch system, we need to model such trains. Give B fragments to define variables and invariants that would specify such trains. You may assume the sets $LOCOS$ and $CARRIAGES$.

   (8 marks)

7. Describe the difference between a *precondition* and a *guard*.

(8 marks)

8. To prove that $f \lhd g \in s \longrightarrow t$, it is sufficient to prove the following lemmas:

   L1 f and g are total functions

   L2 $\mathsf{dom}(f) \cup \mathsf{dom}(g) = s$

   L3 $\mathsf{ran}(f) \subseteq t$ and $\mathsf{ran}(g) \subseteq t$

   Show therefore that if $f \in u \longrightarrow t$, $u \cup \{a\} = s$, and $b \in t$, that $f \lhd \{a \mapsto b\} \in s \longrightarrow t$.
   (8 marks)

9. From the **SimpleBank** machine, we have the following fragments:

...

VARIABLES

$accounts$, $balance$

INVARIANT

$accounts \subseteq ACCOUNT \wedge$
$balance \in accounts \longrightarrow \mathbb{N}$

INITIALISATION

$accounts$, $balance := \{\}$, $\{\}$

...

OPERATIONS

WithDraw ($amount$, $account$) $\widehat{=}$
PRE $amount \in \mathbb{N} \wedge account \in accounts \wedge amount \leq balance$ ($account$)
THEN
$balance := balance \Leftarrow \{ account \mapsto balance$ ($account$) $- amount \}$
END ;

Part of one of the proof obligations is to establish

$$balance(account) - amount \in \mathbb{N}$$

Prove this.

(8 marks)

10. State one principle of software engineering you have learnt, and explain how B does (or does not!) give support to this principle.

(8 marks)