

Monash University

Semester Two 2008 Examination Period

Faculty of Information Technology

EXAM CODES: CSE4213/FIT3013

TITLE OF PAPER: CSE4213 Formal Methods in Software Engineering/
FIT3013 Formal Specification for Software Engineering

EXAM DURATION: 2 hours writing time

READING TIME: 10 minutes

THIS PAPER IS FOR STUDENTS STUDYING AT: Clayton

INSTRUCTIONS FOR CANDIDATES

During an exam, you must not have in your possession, a book, notes, paper, calculator, pencil case, mobile phone or other material/item which has not been authorised for the exam or specifically permitted as noted below. Any material or item on your desk, chair or person will be deemed to be in your possession. You are reminded that possession of unauthorised materials in an exam is a discipline offence under Monash Statute 4.1.

No examination papers are to be removed from the room.

1. Answer **all** questions
2. There are 4 questions
3. Each question is worth 20 marks
4. Total marks 80
5. Calculators are not allowed
6. Use left hand page for rough working; this page will NOT be marked unless explicitly requested.
7. The *Concise Summary of the Event-B mathematical toolkit* is appended to this paper.

AUTHORISED MATERIALS

CALCULATORS: NO

OPEN BOOK: NO

SPECIFICALLY PERMITTED ITEMS: NO

Candidates must complete this section

STUDENT ID

DESK NUMBER

1. (a) Give 3 attributes concerning guards and their role in the Event-B Method. For each attribute, give a corresponding example that demonstrates the attribute.

(6 marks)

(b) Simplify the following predicate transforms

i. $[x := 6] x > y$

ii. $[a : |a' < y \wedge a' := a + 1] a \geq x$

iii. $[y := 2 \times y] y \bmod 2 = 0$

iv. $\neg[v : |s] \neg v = e$

(8 marks)

(c) For each of the following pairs of predicates, state whether the second predicate is stronger or weaker than the first.

i. $n \in \mathbb{N}, n \in \mathbb{N}1$

ii. $n \in \mathbb{N}, n \in \{z | z \in \mathbb{N} \wedge z \bmod 2 = 0\}$

iii. $c \in \text{HOLDEN}, c \in \text{CARS}$

iv. \top, \perp

(4 marks)

(d) i. In a refinement, are the guards stronger or weaker than the corresponding abstract guards?

ii. In a refinement, are the post-conditions stronger or weaker than the corresponding abstract post-conditions?

(2 marks)

2. Read through the following specification (discussed in lectures) and answer the questions at the end of the specification.

An Event-B Specification of ctx_0
Generated Date: 7 Oct 2008 @ 11:57:34 AM

CONTEXT ctx_0

SETS

D

CONSTANTS

n, f, v

AXIOMS

axm1 : $n \in \mathbb{N}$

axm2 : $f \in 1..n \rightarrow D$

axm3 : $v \in \text{ran}(f)$

THEOREMS

thm1 : $n \in \mathbb{N}_1$

END

An Event-B Specification of m_0a
Generated Date: 7 Oct 2008 @ 11:55:22 AM

MACHINE m_0a

SEES ctx_0

VARIABLES

i

INVARIANTS

inv1 : $i \in 1..n$

EVENTS

Initialisation

begin

act1 : $i := 1$

end

search $\hat{=}$

any k

where

grd1 : $k \in 1..n$

grd2 : $f(k) = v$

then

act1 : **skip**

end

END

MACHINE m_1a

REFINES m_0a

SEES ctx_0

VARIABLES

i, j

INVARIANTS

inv1 : $j \in 0 .. n$

inv2 : $v \notin f[1 .. j]$

THEOREMS

thm1 : $v \in f[j + 1 .. n]$

EVENTS

Initialisation

begin

act1 : $i := 1$

act2 : $j := 0$

end

search $\hat{=}$

Refines search

when

grd1 : $f(j + 1) = v$

with

k : $j + 1 = k$

then

act1 : $i := j + 1$

end

progress $\hat{=}$

Which is convergent

when

grd1 : $f(j + 1) \neq v$

then

act1 : $j := j + 1$

end

VARIANT

$n - j$

END

Questions on the preceding specification:

(a) (ctx.0: axm2:) Is f a subset of $\mathbb{N} \times D$ or an element of it?

(2 marks)

(b) (ctx.0: thm1:) If you had to prove $n \in \mathbb{N}1$, what information would you draw upon and why? (You do not have to give a proof.)

(2 marks)

(c) (m.0a: grd2:) Explain in non-mathematical terms what makes guard 2 of event *search* true?

(2 marks)

(d) (m.1a: inv2:/thm1:) Explain in non-mathematical terms what these two predicates imply.

(2 marks)

(e) What is the difference between an invariant and a theorem?

(2 marks)

(f) There is a significant error in the abstract specification. What is it?

(2 marks)

(g) Give the refinement relations between the variables of the abstract specification and the refinement. What is the purpose of the witness variable k (in $m_{1a}:\text{search}$)?

(2 marks)

(h) Explain what deadlock means in the context of an Event-B specification.

(2 marks)

(i) Is deadlock possible for the m_{1a} machine? Why (not)?

(2 marks)

(j) Explain the relationship between the **VARIANT** expression and the statement that *progress* is convergent.

(2 marks)

3. Write an Event B Context that defines a day of the year as day/month. Your context should define two constant sets DAY and MONTH, and a constant function DaysInMonth which, for a given month, defines how many days in that month (ignore leap years).

(20 marks)

4. (a) Refine the following machine to remove the non-determinism (you can use the next page for your answer).

MACHINE Q1

VARIABLES

x

n

INVARIANTS

inv1 : $x \in \mathbb{N}$

inv2 : $n \in \mathbb{N}$

EVENTS

Initialisation

begin

act1 : $x \in \mathbb{N}$

act2 : $n \in \mathbb{N}$

end

E1 $\hat{=}$

when **grd1** : $x = 1$

then **act1** : $n := 1$

end

E2 $\hat{=}$

when **grd1** : $x < 5$

then **act1** : $n := 2$

end

E3 $\hat{=}$

when **grd1** : $x > 3$

then **act1** : $n := 3$

end

E4 $\hat{=}$

when **grd1** : $x \geq 4$

then **act1** : $n := 4$

end

END

(8 marks)

- (b) Reflecting upon the discussion questions offered throughout the semester, describe two issues that for you:
- i. Represents a key advantage of using the Event-B methodology in software engineering
 - ii. Represents a significant disadvantage in using the Event-B methodology in software engineering

(4 marks)

- (c) Give the proof obligation rule for the refinement relation between abstract and concrete variables.

(2 marks)

- (d) Refinements form a lattice moving from the trivially feasible through to the impossibly infeasible. What are the names given to the substitutions that form the fixed points at each end of the lattice? (Indicate which is feasible and infeasible).

(2 marks)

- (e) What is the *conjugate weakest predicate*? Give an example where it is necessary to use the conjugate weakest predicate in order to establish a refinement relation. (Show Event-B specification fragments to support your answer).

(4 marks)

END OF EXAMINATION QUESTIONS