EECS3342-Z Winter 2023		**Name (Print):**	______________
System Specification & Refinement			
Example Exam Questions			
April 16, 2023		PPY Login	______________
Time Limit: 180 Minutes		Signature	______________

This exam contains 5 pages (including this cover page) and 5 problems.

Check to see if any pages are missing.

Do not detach any question pages from the booklet.

Enter **all** requested information on the top of this page before you start the exam, and put your **initials** on the top of every page, in case the pages become separated.

Attempt **all** questions. Answer each question in the boxed space provided.

The following rules apply:

- **NO QUESTIONS DURING THE EXAM.**
- **If a question is ambiguous or unclear, then please write your assumptions and proceed to answer the question.**
- Only writings within the designated answer boxes will be graded. Plan your answers on the sketch paper provided.
- **Write in valid Rodin ASCII syntax** wherever required.
- Where descriptive answers are requested, use complete sentences and paragraphs. Be precise and concise.
- In writing a sequent proof, only one inference rule can be applied at a time.
- Whenever the **ARI** inference rule is used, justify in writing its use.
- **Organize your work**, in a reasonably neat and coherent way, in the space provided. Work scattered all over the page without a clear ordering will receive very little credit.
- **Mysterious or unsupported answers will not receive credit**. A correct answer, unsupported by calculations or explanation will receive no credit; an incorrect answer supported by substantially correct calculations and explanations might still receive partial credit.
- All answers must appear in the boxed areas in this booklet.

Do not write in this table which contains your raw mark scores.

Problem	Points	Score
1	10	
2	10	
3	10	
4	10	
5	20	
Total:	60	

1. Given a model (with static and dynamic parts), what are the factors determining the number sequents generated for invariant preservation?

Solution:

- Number of (old and new) events
- Number of invariant conditions

[of 10 marks]

2. Justify whether or not the following statement is true:

A partial function is always a total function.

Solution:

- The statement is false.
- A partial function $f \in S \pfun T$ may have its domain $\text{dom}(f) \subset S$, which violates the requirement of a function being total (e.g., $\text{dom}(f) = S$).

[of 10 marks]

3. Can the left sequent below be transformed to the two right sequents via `OR_L`?

$$\boxed{\begin{array}{l} a+1>5 \lor a+1=5 \\ \vdash \\ a>0 \end{array}} \;\; ?? \;\; \begin{array}{l} \boxed{\begin{array}{l} a>0 \\ \vdash \\ a+1>5 \end{array}} \\ \\ \boxed{\begin{array}{l} a>0 \\ \vdash \\ a+1=5 \end{array}} \end{array}$$

Solution:

- No.
- By applying `OR_L`, the two disjuncts $a + 1 > 5$ and $a + 1 = 5$ should appear as separate antecedents, not separate goals. Also, the goal $a > 0$ should not be transformed to a hypothesis.

[of 10 marks]

4. Consider the following action which intends to update the balance function $b \in ACCOUNT \pfun \mathbb{Z}$:

b(a) := b(a) + v

In valid Rodin ASCII syntax, rewrite the right-hand side of "becomes" operator using set and/or relational operators.

Solution:

- Acceptable answer 1: `a |-> b(a) + v  ({a} <<| b)`
- Acceptable answer 2: `b <+ {a |-> b(a) + v}`

[of 10 marks]

5. Consider the following models of the bridge controller system:

m0: Initial Model

constants: d

axioms:
axm0_1 : $d \in \mathbb{N}$
axm0_2 : $d > 0$

variables: n

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \leq d$

init
begin
$n := 0$
end

ML_out
when
$n < d$
then
$n := n + 1$
end

ML_in
when
$n > 0$
then
$n := n - 1$
end

m1: First Refinement

constants: d

axioms:
axm0_1 : $d \in \mathbb{N}$
axm0_2 : $d > 0$

variables: a, b, c

invariants:
inv1_1 : $a \in \mathbb{N}$
inv1_2 : $b \in \mathbb{N}$
inv1_3 : $c \in \mathbb{N}$
inv1_4 : $a + b + c = n$
inv1_5 : $a = 0 \lor c = 0$

variants:
$2 \cdot a + b$

init
begin
$a := 0$
$b := 0$
$c := 0$
end

ML_out
when
$a + b < d$
$c = 0$
then
$a := a + 1$
end

ML_in
when
$c > 0$
then
$c := c - 1$
end

IL_in
when
$a > 0$
then
$a := a - 1$
$b := b + 1$
end

IL_out
when
$b > 0$
$a = 0$
then
$b := b - 1$
$c := c + 1$
end

Formulate and prove **ML_in/GRD**.

Solution:

$$\boxed{\begin{array}{l} d \in \mathbb{N} \\ d > 0 \\ n \in \mathbb{N} \\ n \leq d \\ a \in \mathbb{N} \\ \underline{b \in \mathbb{N}} \\ c \in \mathbb{N} \\ \underline{a + b + c = n} \\ \underline{a = 0 \lor c = 0} \\ \underline{c > 0} \\ \vdash \\ n > 0 \end{array}} \ \textbf{MON} \ \boxed{\begin{array}{l} b \in \mathbb{N} \\ a + b + c = n \\ \underline{a = 0 \lor c = 0} \\ c > 0 \\ \vdash \\ n > 0 \end{array}} \ \textbf{OR\_L} \left\{ \begin{array}{l} \boxed{\begin{array}{l} b \in \mathbb{N} \\ \underline{a} + b + c = n \\ \underline{a = 0} \\ c > 0 \\ \vdash \\ n > 0 \end{array}} \ \textbf{EQ\_LR}, \textbf{MON} \ \boxed{\begin{array}{l} b \in \mathbb{N} \\ \underline{0 + b + c = n} \\ c > 0 \\ \vdash \\ n > 0 \end{array}} \ \textbf{ARI} \ \boxed{\begin{array}{l} \underline{b \in \mathbb{N}} \\ \underline{b + c = n} \\ c > 0 \\ \vdash \\ n > 0 \end{array}} \ \textbf{ARI} \ \boxed{\begin{array}{l} \underline{c \leq n} \\ \underline{c > 0} \\ \vdash \\ n > 0 \end{array}} \ \textbf{ARI} \ \boxed{\begin{array}{l} n > 0 \\ \vdash \\ n > 0 \end{array}} \ \textbf{HYP} \\ \\ \boxed{\begin{array}{l} b \in \mathbb{N} \\ a + b + \underline{c} = n \\ \underline{c = 0} \\ \underline{c} > 0 \\ \vdash \\ n > 0 \end{array}} \ \textbf{EQ\_LR} \ \boxed{\begin{array}{l} b \in \mathbb{N} \\ a + b + \underline{0} = n \\ \underline{c = 0} \\ \underline{0} > 0 \\ \vdash \\ n > 0 \end{array}} \ \textbf{EQ\_LR}, \textbf{MON} \ \boxed{\begin{array}{l} \underline{0 > 0} \\ \vdash \\ n > 0 \end{array}} \ \textbf{ARI} \ \boxed{\begin{array}{l} \bot \\ \vdash \\ n > 0 \end{array}} \ \textbf{FALSE\_L} \end{array} \right.$$

It is also expected that each application of **ARI** is justified.

[of 20 marks]

This is a blank page for sketching purpose. You may detach it from the exam booklet.
Do **not** detach other question pages from the exam booklet.

This is a blank page for sketching purpose. You may detach it from the exam booklet.
Do **not** detach other question pages from the exam booklet.