

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  $f \in S \leftrightarrow T$  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?

$$\begin{array}{ccc}
 \boxed{a + 1 > 5 \vee a + 1 = 5} & \text{??} & \boxed{a > 0} \\
 \vdash & & \vdash \\
 \boxed{a > 0} & & \boxed{a + 1 > 5} \\
 & & \\
 & & \boxed{a > 0} \\
 & & \vdash \\
 & & \boxed{a + 1 = 5}
 \end{array}$$

**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  $b \in \text{ACCOUNT} \rightarrow \mathbb{Z}$ :

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

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

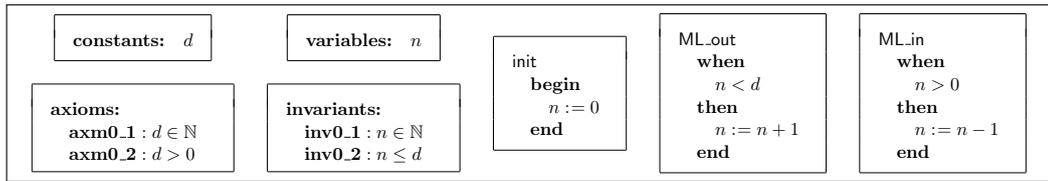
**Solution:**

- Acceptable answer 1:  $\mathbf{a} \mid\text{-}\> \mathbf{b(a)} + \mathbf{v} \quad (\{\mathbf{a}\} \ll\mid \mathbf{b})$
- Acceptable answer 2:  $\mathbf{b} \text{ <+ } \{\mathbf{a} \mid\text{-}\> \mathbf{b(a)} + \mathbf{v}\}$

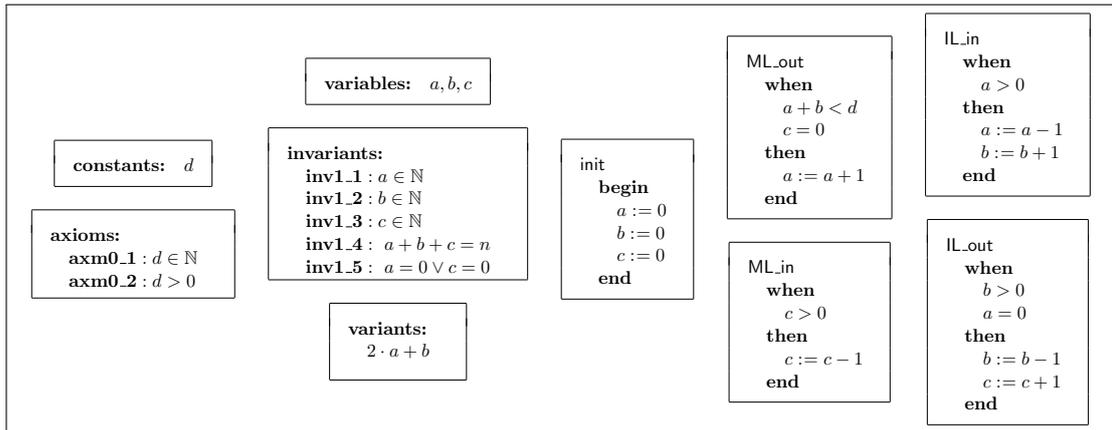
[      of 10 marks]

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

**m0: Initial Model**



**m1: First Refinement**



Formulate and prove **ML\_in/GRD**.

**Solution:**

The proof tree for **ML\_in/GRD** is as follows:

- Left side (Axioms and Invariants):**
  - Box 1:  $d \in \mathbb{N}, d > 0, n \in \mathbb{N}, n \leq d, a \in \mathbb{N}, b \in \mathbb{N}, c \in \mathbb{N}, a + b + c = n, a = 0 \vee c = 0, c > 0, \top, n > 0$
  - Box 2:  $b \in \mathbb{N}, a + b + c = n, a = 0 \vee c = 0, c > 0, \top, n > 0$
- Logical Rules:**
  - MON:** Connects Box 1 and Box 2.
  - OR.L:** Connects Box 2 to two parallel branches.
- Top Branch (Successful):**
  - Box 3:  $b \in \mathbb{N}, a + b + c = n, a = 0, c > 0, \top, n > 0$
  - Box 4:  $b \in \mathbb{N}, 0 + b + c = n, c > 0, \top, n > 0$
  - Box 5:  $b \in \mathbb{N}, b + c = n, c > 0, \top, n > 0$
  - Box 6:  $c \leq n, c > 0, \top, n > 0$
  - Box 7:  $n > 0, \top, n > 0$
  - Rules: **EQ\_LR, MON** (2-3), **ARI** (3-4), **ARI** (4-5), **ARI** (5-6), **HYP** (6-7).
- Bottom Branch (Fails):**
  - Box 8:  $b \in \mathbb{N}, a + b + c = n, c = 0, c > 0, \top, n > 0$
  - Box 9:  $b \in \mathbb{N}, a + b + 0 = n, c = 0, 0 > 0, \top, n > 0$
  - Box 10:  $0 > 0, \top, n > 0$
  - Box 11:  $\perp, \top, n > 0$
  - Rules: **EQ\_LR** (8-9), **EQ\_LR, MON** (9-10), **ARI** (10-11), **FALSE.L** (11-12).

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

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.