EECS3342-E Fall 2025 **Name (Print):** _____
System Specification & Refinement
Example Exam Questions
December 11, 2025 PPY Login _____
Time Limit: 180 Minutes Signature _____

This exam contains 8 pages (including this cover page) and 6 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 <u>one</u> inference rule can be applied at a time.
  Here is the **<u>only</u>** exception: you can write `EQ_LR` or `EQ_RL`, followed by `MON`, as a single step.
- 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	
6	30	
Total:	90	

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`?

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

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 $b \in ACCOUNT \pfun \mathbb{Z}$:

$$\text{b(a)} := \text{b(a)} + \text{v}$$

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

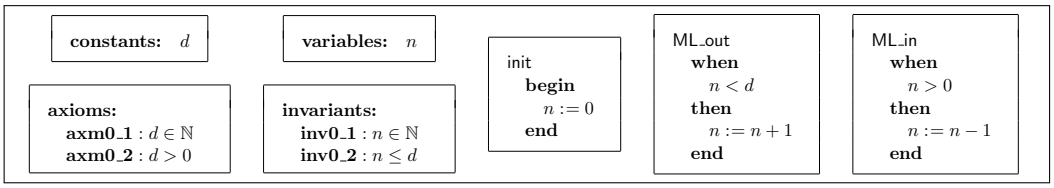
Solution:

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

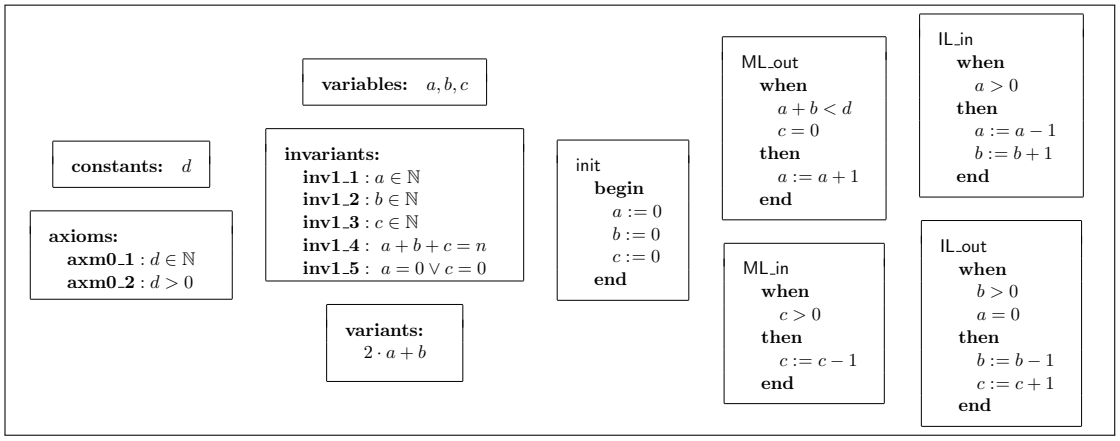
[of 10 marks]

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

m0: Initial Model



m1: First Refinement



Formulate and prove **ML_in/GRD**.

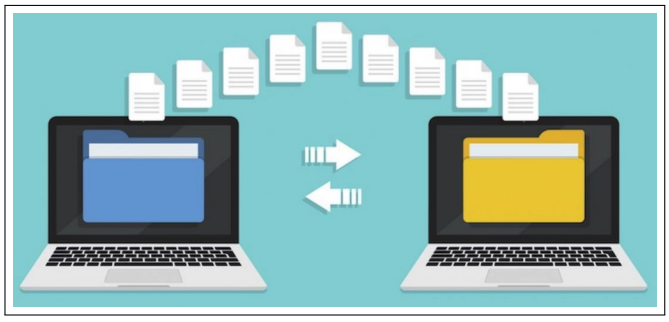
Solution:

$$\frac{\begin{array}{l} d \in \mathbb{N} \\ d > 0 \\ n \in \mathbb{N} \\ n \leq d \\ a \in \mathbb{N} \\ \underline{b \in \mathbb{N}} \\ c \in \mathbb{N} \\ \underline{a + b + c = n} \\ \underline{a = 0 \vee c = 0} \\ \underline{c > 0} \\ \vdash \\ n > 0 \end{array}}{\mathbf{MON}\ \dfrac{\begin{array}{l} b \in \mathbb{N} \\ a + b + c = n \\ \underline{a = 0 \vee c = 0} \\ c > 0 \\ \vdash \\ n > 0 \end{array}}{\mathbf{OR\_L}\ \begin{cases} \dfrac{\begin{array}{l} b \in \mathbb{N} \\ \underline{a} + b + c = n \\ \underline{a = 0} \\ c > 0 \\ \vdash \\ n > 0 \end{array}}{\mathbf{EQ\_LR, MON}\ \dfrac{\begin{array}{l} b \in \mathbb{N} \\ 0 + b + c = n \\ c > 0 \\ \vdash \\ n > 0 \end{array}}{\mathbf{ARI}\ \dfrac{\begin{array}{l} \underline{b \in \mathbb{N}} \\ b + c = n \\ c > 0 \\ \vdash \\ n > 0 \end{array}}{\mathbf{ARI}\ \dfrac{\begin{array}{l} \underline{c \leq n} \\ c > 0 \\ \vdash \\ n > 0 \end{array}}{\mathbf{ARI}\ \dfrac{\begin{array}{l} n > 0 \\ \vdash \\ n > 0 \end{array}}{\mathbf{HYP}}}}} \\ \dfrac{\begin{array}{l} b \in \mathbb{N} \\ a + b + \underline{c} = n \\ \underline{c = 0} \\ \underline{c} > 0 \\ \vdash \\ n > 0 \end{array}}{\mathbf{EQ\_LR}\ \dfrac{\begin{array}{l} b \in \mathbb{N} \\ a + b + \underline{0} = n \\ \underline{c = 0} \\ \underline{0} > 0 \\ \vdash \\ n > 0 \end{array}}{\mathbf{EQ\_LR, MON}\ \dfrac{\begin{array}{l} \underline{0 > 0} \\ \vdash \\ n > 0 \end{array}}{\mathbf{ARI}\ \dfrac{\begin{array}{l} \bot \\ \vdash \\ n > 0 \end{array}}{\mathbf{FALSE\_L}}}} \end{cases}}}$$

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

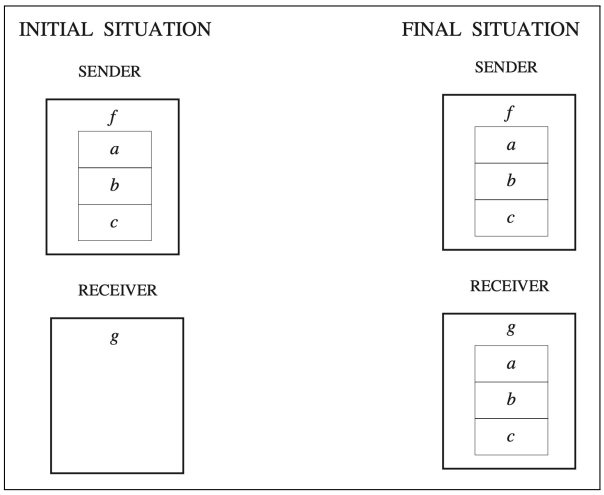
[of 20 marks]

6. You are required to implement a system for transmitting files between agents over a computer network.



Here are the list of intended functionalities of the system:

REQ1	The protocol ensures the copy of a file from the sender to the receiver.
REQ2	The file is supposed to be made of a sequence of items.
REQ3	The file is sent piece by piece between the two sites.



Consider the initial model (m_0) for the above system which only addresses the above **REQ1**: a file is transmitted from the sender to the receiver.

This is the most abstract model, as each file is transmitted from the sender to the receiver *synchronously* and *instantaneously*. That is, the transmission process is abstracted away.

The static part of m_0 formulates each file to be transmitted as a sequence of data items (where n denotes the number of items in the file to be transmitted, and f represents the file to be transmitted from the sender's end):

sets: $D, BOOLEAN$ | **constants:** n, f

axioms:
- **axm0_1** : $n > 0$
- **axm0_2** : $f \in 1 \mathinner{..} n \rightarrow D$
- **axm0_3** : $BOOLEAN = \{TRUE, FALSE\}$

The dynamic part of m_0 contains the following state space (where g represents parts of the file that has been received so far at the receiver's end, and b denotes whether or not the transmission is completed):

variables: g, b

invariants:
- **inv0_1a** : $g \in 1 \mathinner{..} n \nrightarrow D$
- **inv0_1b** : $b \in BOOLEAN$
- **inv0_2** : ??
- **inv0_3** : ??

(a) In valid Rodin syntax, formulate **inv0_2**, which intends to specify what happens **before** the transmission.

Solution:

```
b = false => g = {}
```

[of 5 marks]

(b) In valid Rodin syntax, formulate **inv0_3**, which intends to specify what happens **after** the transmission.

Solution:

```
b = true => g = f
```

[of 5 marks]

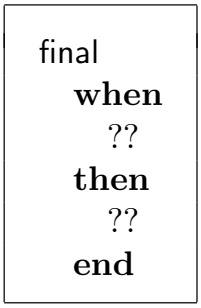
(c) When the system is first launched, nothing has been transmitted to the receiver. Accordingly, in valid Rodin syntax, specify actions of the `init` event.

Solution:

```
g := {}
b := false
```

[of 5 marks]

(d) There is only one non-initialization event, `final`, due to the assumed abstraction that the transmission is synchronous and instantaneous:



The `final`, when enabled, is meant to transmit, instantaneously, the entire file from the sender side to the receiver side upon the event's occurrence.

In valid Rodin syntax, specify the guard(s) and action(s) of the `final` event.

Solution:

- Guard: `b = false`
- Actions:

```
g := f
b := true
```

[of 5 marks]

(e) Formulate the proof obligation `final/inv0_1a/INV`.

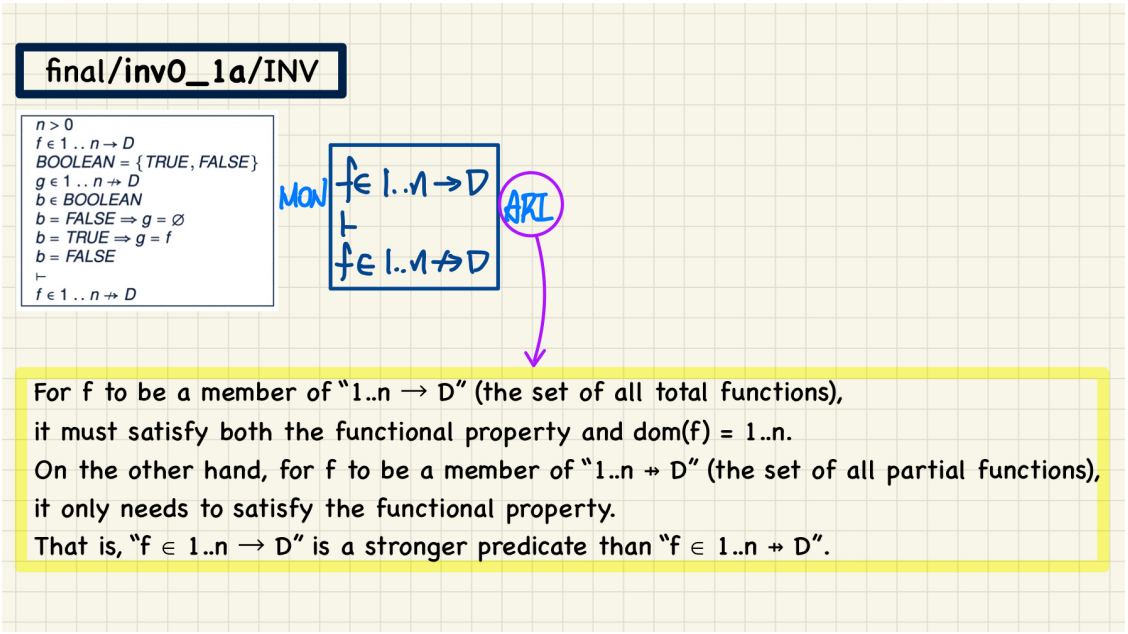
Solution:

$$\frac{\begin{array}{l} n > 0 \\ f \in 1\,..\,n \to D \\ BOOLEAN = \{TRUE, FALSE\} \\ g \in 1\,..\,n \nrightarrow D \\ b \in BOOLEAN \\ b = FALSE \Rightarrow g = \varnothing \\ b = TRUE \Rightarrow g = f \\ b = FALSE \end{array}}{f \in 1\,..\,n \nrightarrow D}\ \textbf{final/inv0\_1a/INV}$$

[of 5 marks]

(f) Show, formally, whether or not `final/inv0_1a/INV` is provable.

Solution:



[of 5 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.