EECS4315-Z Winter 2023
Mission Critical Systems
Example Exam Questions

Name (Print): _____

PPY Login _____

Signature _____

This exam contains 5 pages (including this cover page) and 2 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 write your assumptions and proceed to answer the question.**
- Do **not** write your answers in the questions booklet. **Only answers written in the separate answers booklet will be graded.**
- Do **not** sketch your work in the answers booklet. **Only sketch on the blank pages attached to the questions booklet.**
- At the end of the exam, be sure to submit **all** the following: **1)** Exam questions booklet; **2)** Exam answers booklet(s); and **3)** Data sheet.
  Each one of the above submissions **must** be written with your **full name** and **student number**. **If any of the above submissions is missing, your exam will not be graded.**
- Where descriptive answers are requested, use complete sentences and paragraphs. Be precise and concise.
- **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.

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

Problem	Points	Score
1	75	
2	25	
Total:	100	

1. Consider the following algorithm which computes the maximum value from an input tuple of integers:

```
--------------------------- MODULE findMax ---------------------------
EXTENDS Integers, Sequences, TLC
CONSTANT input
\* defines LI and invariant here
I(i, result) == \A j \in 1..i-1: result >= input[j]
V(i, inp) == Len(inp) - i + 1
(*
--algorithm FindMax {
  variables result = input[1], i = 1, variant_pre = 0, variant_post = 0;
  {
    assert Len(input) > 0; \* precondition
    assert I(i, result); \* invariant
    while (i =< Len(input)) {
      variant_pre := V(i, input);

      if (input[i] > result) { result := input[i] };
      i := i + 1;

      variant_post := V(i, input);
      assert variant_post >= 0;
      assert variant_post < variant_pre;
      assert I(i, result); \* invariant
    };
    \* postcondition
    assert \A j \in 1..Len(input): result >= input[j]
  }
}
*)
```

(a) State formally the obligation for proving that the loop invariant is established.
Requirement. Where a predicate is stated, it must be written in math form (translated from the given PlusCal syntax).

[of 10 marks]

(b) Prove or disprove the stated proof obligation from Part (a).
Requirement. Calculation and proof steps should be presented in the equational style. Each step should be as *atomic* as possible: do not skip or perform multiple steps at a time.

[of 20 marks]

(c) State formally the obligation for proving that the loop invariant is maintained.
Requirement. Where a predicate is stated, it must be written in math form (translated from the given PlusCal syntax).

[of 10 marks]

(d) Prove or disprove the stated proof obligation from Part (c).
Requirement. Calculation and proof steps should be presented in the equational style. Each step should be as *atomic* as possible: do not skip or perform multiple steps at a time.

[of 20 marks]

(e) Refer to the algorithm `findMax` at the start of this question. Consider a change of the loop invariant to:

```
\A j \in 1..i: result >= input[j]
```

Say the algorithm is run on an input tuple `<<20, 10, 40, 30>>`. Describe how a loop invariant violation, if any, will occur.

[of 15 marks]

2. Consider the following claim relating two path satisfactions:

$$\pi \models \mathbf{G}\ \phi \iff \pi \models \neg\ (\mathbf{F}\ \neg\phi)$$

where π is any path that is valid for the model (i.e., some LTS) in question, and ϕ is any arbitrary LTL formula that is syntactically correct. Prove or disprove the above claim.

[of 25 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.