CIS 500: Software Foundations

Midterm II

November 7, 2019

Name (printed): ________________________________

Username (PennKey login id): ________________________________

My signature below certifies that I have complied with the University of Pennsylvania’s Code of Academic Integrity in completing this examination.

Signature: ________________________________ Date: ________________________________

Directions: This exam contains both standard and advanced-track questions. Questions with no annotation are for both tracks. Other questions are marked “Standard Track Only” or “Advanced Track Only.”

Do not waste time (or confuse the graders) by answering questions intended for the other track. To ensure, please look for the questions for the other track as soon as you begin the exam and cross them out!

Mark the box of the track you are following.

☐ Standard ☐ Advanced

Before beginning the exam, please write your PennKey (login ID) at the top of each even-numbered page (so that we can find things if a staple fails!).
1 (11 points) Translate each of the following informal specifications into a precise formal specification using a Hoare triple. For example, if the informal specification is “The command c increases the value of X by 1,” an appropriate formal specification might be \(\forall m, \{X = m\} \ c \ \{X = m + 1\}\).

To reduce clutter, please use informal paper-and-pencil notation when writing assertions (e.g., write \(X = 0\) rather than \(\text{fun st} => \text{st X} = 0\)).

If you use Coq variables in your pre- and post-conditions (like \(m\) above), make sure that you write an explicit quantifier before the precondition.

1.1 The command c swaps the values of X and Y.

\[
\{X = X'\} \ c \ \{X' = X, Y = Y'\}
\]

1.2 The command c sets Z to be the maximum of X and Y.

\[
\{X = X', Y = Y'\} \ c \ \{Z = \max(X', Y')\}
\]
1.3 When $Y$ is non-zero, $c$ computes $X / Y$ and stores the result in $Z$.

1.4 The command $c$ diverges if the initial value of $X$ is strictly smaller than the initial value of $Y$. 
(12 points) For each of the following pairs of programs, mark the box indicating whether or not the programs are equivalent according to $cequiv$. If the programs are not equivalent, give a counterexample—i.e., a starting state on which they behave differently.

Note that some of these definitions are actually “templates” for commands (e.g., ?? is implicitly parameterized by a natural number $n$ and ?? by an arbitrary boolean expression $b$). For these you should make sure that the programs are equivalent for any choice of the parameter.

2.1

\begin{align*}
X & ::= n; \\
& \text{WHILE } \neg(X = 0) \text{ DO} \\
& \hspace{1cm} X ::= X - 1 \\
& \text{END} \\
& \text{SKIP}
\end{align*}

\begin{tabular}{c c}
\(\square\) Equivalent & \(\square\) Not Equivalent \\
\end{tabular}

Counterexample (if “Not Equivalent”):

2.2

\begin{align*}
& \text{SKIP} \\
& T ::= X; \ X ::= Y; \ Y ::= T; \\
& T ::= X; \ X ::= Y; \ Y ::= T
\end{align*}

\begin{tabular}{c c}
\(\square\) Equivalent & \(\square\) Not Equivalent \\
\end{tabular}

Counterexample (if “Not Equivalent”):
2.3

\[
\text{WHILE } b \text{ DO} \\
\quad Y ::= X ;; \\
\quad Z ::= Y \times Z \\
\text{END}
\]

\[
\text{Y ::= X ;;} \\
\text{WHILE } b \text{ DO} \\
\quad Z ::= Y \times Z \\
\text{END}
\]

\[\square\, \text{Equivalent} \quad \square\, \text{Not Equivalent}\]

Counterexample (if “Not Equivalent”):

2.4

\[
\text{WHILE } \neg (X = Y) \text{ DO} \\
\quad X ::= X + 1 \\
\text{END}
\]

\[
\text{X ::= X - 1 ;;} \\
\text{WHILE } \neg (X = Y) \text{ DO} \\
\quad X ::= X + 1 \\
\text{END}
\]

\[\square\, \text{Equivalent} \quad \square\, \text{Not Equivalent}\]

Counterexample (if “Not Equivalent”):
In order to verify an Imp program that contains a loop—either with a direct proof using the Hoare Logic rules (page ?? in the appendix) or by decorating it with assertions (page ?? in the appendix)—we need to find a loop invariant that also serves as a valid pre- and post-condition for the loop. That is, we need to find an assertion that satisfies three conditions:

(a) It must be weak enough to be implied by the loop’s precondition.

(b) It must be strong enough to imply the program’s postcondition (given that the loop guard evaluates to false).

(c) It must be preserved by each iteration of the loop (given that the loop guard evaluates to true).

For example, the assertion True is not a useful invariant for the following decorated program because it fails to imply the needed postcondition:

(1) \{\{ X = m \land Y = n \}\} \implies \text{OK} - (1) \implies (2)
(2) \{\{ \text{True} \}\}

WHILE \neg(X = 0) DO
(3) \{\{ \text{True} \land X \neq 0 \}\} \implies \text{OK} - (3) \implies (4)
(4) \{\{ \text{True} \}\}
    Y ::= Y - 1;
(5) \{\{ \text{True} \}\}
    X ::= X - 1
(6) \{\{ \text{True} \}\}

END
(7) \{\{ \text{True} \land \neg(X \neq 0) \}\} \implies \text{WRONG!} - (7) \text{doesn’t imply (8)}
(8) \{\{ Y = n - m \}\}

For each of the proposed invariants for the decorated WHILE loop at the top of the next page, mark all of the correct implications—e.g., for the example loop on this page and the proposed invariant True, you would mark (a) and (c) but not (b).
Decorated loop:

\[
\begin{align*}
\{ \{ X = n \land Y = 0 \} \} & \implies (a) \\
\{ \{ \text{invariant} \} \} \\
\textbf{WHILE} \neg(X = 0) \textbf{DO} \\
\{ \{ \text{invariant} \land X \neq 0 \} \} & \implies (c) \\
\{ \{ \ldots \} \} \\
X & := X - 1 ;; \\
Y & := Y + 1 \\
\{ \{ \text{invariant} \} \} \\
\textbf{END} \\
\{ \{ \text{invariant} \land (X = 0) \} \} & \implies (b) \\
\{ \{ Y = n \} \} \\
\end{align*}
\]

Possible invariants:

3.1 \hspace{0.5cm} X \leq n

- (a) Precondition implies invariant
- (b) Invariant and negated guard imply postcondition
- (c) Invariant is preserved by the loop body

3.2 \hspace{0.5cm} Y - X > 0

- (a) Precondition implies invariant
- (b) Invariant and negated guard imply postcondition
- (c) Invariant is preserved by the loop body

3.3 \hspace{0.5cm} Y > 0

- (a) Precondition implies invariant
- (b) Invariant and negated guard imply postcondition
- (c) Invariant is preserved by the loop body

3.4 \hspace{0.5cm} X + Y = n \land X \leq n

- (a) Precondition implies invariant
- (b) Invariant and negated guard imply postcondition
- (c) Invariant is preserved by the loop body

3.5 \hspace{0.5cm} \text{False}

- (a) Precondition implies invariant
- (b) Invariant and negated guard imply postcondition
- (c) Invariant is preserved by the loop body
The Imp program below calculates the sum of the natural numbers up to \( n \). Add appropriate annotations to the program in the provided spaces to show that the Hoare triple given by the outermost pre- and post-conditions is valid. Please be completely precise and pedantic in the way you apply the Hoare rules—i.e., write out assertions in exactly the form given by the rules, rather than logically equivalent ones. The provided blanks have been constructed so that, if you work backwards from the end of the program, you should only need to use the rule of consequence in the places indicated with \( \Rightarrow \).

The implication steps in your decorations may rely (silently) on all the usual rules of natural-number arithmetic.

The rules of Hoare logic and the rules for well-formed decorated programs can be found on pages 3 and ?? of the appendix.

\[
\{\{ X = n \}\} \Rightarrow
\{
Y := 0
\{\}
\}
\{
Z := 0
\{\}
\}
\{
\WHILE \neg (Z = X) \DO
\{\}
\{\}
\{Z := 1 + Z\}
\{\}
\{Y := Y + Z\}
\{\}
\END
\{\}
\{2 \times Y = n \times (1 + n)\}
\]
The two following programs compute the sum of natural numbers from 0 to \( n \) in different ways:

```
Definition sum_loop : com :=
  WHILE ~(C = 0) DO
    T ::= T + C;;
    C ::= C - 1
  END.

Definition sum_closed : com :=
  T ::= T + (C * (C + 1)) / 2;;
  C ::= 0.
```

The first program \((\text{sum\_loop})\) calculates the sum incrementally, adding \( n \) (the initial value of \( C \)) to \( T \), then adding \( n-1 \) to \( T \), and so on. The second \((\text{sum\_closed})\) just statically adds the closed form of the sum from 0 to \( n \) to \( T \) (and sets \( C \) to 0).

Note that, in both cases, we add the sum to the initial value of \( T \) rather than setting \( T \) to the sum. This makes the reasoning below a bit simpler. Also, note that we have technically added division to the IMP language here. You can assume that it behaves like normal integer division, where the result is rounded down (details like rounding and how division by zero behaves should not matter here).

On the next page, write a careful, informal proof of (one direction of) the equivalence between these programs. Be sure to spell out any induction hypotheses explicitly.

The following lemma may help simplify some calculation in your proof:

```
Lemma sn_sum :
  forall n, S n + ((n * (n + 1)) / 2) = (S n * (S n + 1)) / 2.
```

Additionally, to keep the proof smaller, if you have a command with multiple assignments sequenced together like so...

```
  st = [ X ::= 2;; Y ::= 2 + X;; c ]=> st'
```

...you may derive in one step that:

```
  (X !-> 2; Y !-> 4; st) = [ c ]=> st'
```

Normally you would arrive at this conclusion by multiple inversions of the first evaluation relation, but this level of detail is not necessary.
It is helpful to phrase the theorem in a slightly odd way, so that we can prove it by induction on \( n \) instead of induction on \( \text{ceval} \) derivations (this would also work, but the proof would be a bit heavier):

\[
\text{Theorem sum_loop_implies_sum_closed} : \\
\forall n : \text{nat}, \\
\forall \text{st st'} : \text{state}, \\
\text{st C = n -> st =} \sum\text{loop} \implies \text{st -}\rightarrow \\
\text{st =} \sum\text{closed} \implies \text{st'.}
\]

\text{Proof:} By induction on \( n \).

\text{Complete the proof...}
The version of Hoare Logic that we've studied in class focuses on partial correctness—i.e., its specifications (“Hoare triples”) have the form “if we start command $c$ in a state satisfying precondition $P$, and if $c$ terminates in a state $st'$, then $st'$ satisfies postcondition $Q$.”

There is another variant of Hoare Logic, called total-correctness Hoare Logic, whose triples make a stronger claim about termination: “if we start command $c$ in a state satisfying $P$, then $c$ is guaranteed to terminate in some state $st'$ that satisfies $Q$.” This stronger form of Hoare triple is defined as follows:

\[
\text{Definition } \text{tc_hoare_triple } (P : \text{Assertion}) (c : \text{com}) (Q : \text{Assertion}) : \text{Prop} := \\
\forall st, \\
P st \rightarrow \\
\exists st', \\
\text{st} = [c] \Rightarrow st' \\
\land \ Q \text{ st'}.
\]

We write total-correctness Hoare triples with \([\ldots]\) brackets around the pre- and post-conditions, to distinguish them from our familiar partial-correctness triples.

\text{Notation } "[[ P ]] c [[ Q ]]" := (tc_hoare_triple P c Q)
On the left below are a number of ordinary (partial correctness) Hoare triples; on the right are analogous total-correctness triples. Indicate whether each triple is valid or invalid in the appropriate sense by checking the corresponding box. Note that the commands and assertions are the same between the left and right parts of each subproblem—only the shape of the brackets around the assertions (i.e., whether we are talking about partial or total correctness) is different.

**Partial correctness:**

```
{{ True }}
WHILE 1 <= X DO
    X ::= X - 1 
END
{{ X = 0 }}
```

- [ ] Valid
- [ ] Invalid

**Total correctness:**

```
[[ True ]]
WHILE 1 <= X DO
    X ::= X - 1 
END
[[ X = 0 ]]
```

- [ ] Valid
- [ ] Invalid

**Partial correctness:**

```
{{ True }}
WHILE 1 <= X DO
    X ::= X + 1 
END
{{ True }}
```

- [ ] Valid
- [ ] Invalid

**Total correctness:**

```
[[ True ]]
WHILE 1 <= X DO
    X ::= X + 1 
END
[[ True ]]
```

- [ ] Valid
- [ ] Invalid

**Partial correctness:**

```
{{ X = 0 }}
WHILE 1 <= X DO
    X ::= X + 1 
END
{{ True }}
```

- [ ] Valid
- [ ] Invalid

**Total correctness:**

```
[[ X = 0 ]]
TEST X = 5 THEN
    WHILE true DO SKIP END
ELSE
    SKIP
FI
[[ X = 3 ]]
```

- [ ] Valid
- [ ] Invalid

**Total correctness:**

```
[[ X = 5 ]]
TEST X = 5 THEN
    WHILE true DO SKIP END
ELSE
    SKIP
FI
[[ X = 3 ]]
```

- [ ] Valid
- [ ] Invalid
Are the following propositions true? If so, check Yes. If not, check No and give a counterexample.

\(\forall (c : \text{com}), \ [[\text{False}]] c \ [\text{True}]\)

\[\square \ Yes \quad \square \ No\]

*Counterexample (if appropriate):*

\(\forall (c : \text{com}), \ [[\text{True}]] c \ [\text{True}]\)

\[\square \ Yes \quad \square \ No\]

*Counterexample (if appropriate):*

\(\forall P, \ [[P]] \text{WHILE true DO SKIP END } [[P]]\)

\[\square \ Yes \quad \square \ No\]

*Counterexample (if appropriate):*

\(\forall P, \ [[P]] \text{WHILE false DO SKIP END } [[P]]\)

\[\square \ Yes \quad \square \ No\]

*Counterexample (if appropriate):*
7 (10 points) Recall the definition of what it means for a term \( t \) to be a normal form of a relation \( R \):

\[
\text{Definition normal\_form} \{ X : \text{Type} \} (R : \text{relation} X) (t : X) : \text{Prop} :=
\neg \exists t', R t t'.
\]

7.1 Give a complete and precise description, in English, of all the Imp arithmetic expressions \( a : \text{aexp} \) that are normal forms for the small-step reduction relation on arithmetic expressions (\text{astep}, see page ?? in the appendix)—i.e., for which the proposition \text{normal\_form} (\text{astep} st) a holds for all states \( st \).

7.2 Give a complete and precise description of all the Imp commands \( c \) and states \( st \) such that the pair \((c, st)\) is a normal form for the cstep relation (page ?? in the appendix).

7.3 Define informally what it means for a step relation to be normalizing.

7.4 Give an informal definition of strong progress.

7.5 Does strong progress imply termination?

\( \square \) Yes \quad \square \) No
Use this space for scratch work that you don't want graded. If you write something here that you do want graded, make sure there is a very clear pointer from the earlier page where you ran out of space.
For Reference

Imp

Arithmetic expressions (extended with division) and boolean expressions:

```ocaml
Fixpoint aeval (st : state) (a : aexp) : nat :=
    match a with
    | ANum n => n
    | AId x => st x
    | APlus a1 a2 => (aeval st a1) + (aeval st a2)
    | AMinus a1 a2 => (aeval st a1) - (aeval st a2)
    | AMult a1 a2 => (aeval st a1) * (aeval st a2)
    | ADiv a1 a2 => (aeval st a1) / (aeval st a2)
    end.

Fixpoint beval (st : state) (b : bexp) : bool :=
    match b with
    | BTrue => true
    | BFalse => false
    | BEq a1 a2 => (aeval st a1) =? (aeval st a2)
    | BLe a1 a2 => (aeval st a1) <=? (aeval st a2)
    | BNot b1 => negb (beval st b1)
    | BAnd b1 b2 => andb (beval st b1) (beval st b2)
    end.
```

Commands:

```
-------------- (E_Skip)
st = [ SKIP ] => st

-------------- (E_Ass)
aeval st a1 = n
st = [ x := a1 ] => (x !-> n ; st)

-------------- (E_Seq)
st = [ c1 ] => st'
st' = [ c2 ] => st''

-------------- (E_IfTrue)
beval st b1 = true
st = [ c1 ] => st'

-------------- (E_IfFalse)
beval st b1 = false
st = [ c2 ] => st'
```

1
beval st b = false

----------------------------- (E_WhileFalse)
st = [ WHILE b DO c END ] => st

beval st b = true

st = [ c ] => st

st' = [ WHILE b DO c END ] => st''

----------------------------- (E_WhileTrue)

st = [ WHILE b DO c END ] => st''

### Equivalence

**Definition**

\[
\text{cequiv} \ (c_1 \ c_2 : \text{com}) : \text{Prop} := \\
\forall (st \ st') : \text{state}, \\
\left( st = [ c_1 ] => st' \right) \leftrightarrow \left( st = [ c_2 ] => st' \right).
\]

### Hoare triples

**Definition**

\[
\text{Assertion} := \text{state} -> \text{Prop}.
\]

**Definition**

\[
\text{assert_implies} \ (P \ Q : \text{Assertion}) : \text{Prop} := \\
\forall st, P st \rightarrow Q st.
\]

**Notation**

\[
P =>> Q := (\text{assert_implies} \ P \ Q)
\]

**Definition**

\[
\text{hoare_triple} \ (P : \text{Assertion}) (c : \text{com}) (Q : \text{Assertion}) : \text{Prop} := \\
\forall st st', \\
\left( st = [ c ] => st' \right) \rightarrow \\
P st \rightarrow \\
Q st'.
\]

**Notation**

\[
\text{hoare_triple} \ P \ c \ Q := (\text{hoare_triple} \ P \ c \ Q)
\]
Hoare logic

---------------------------------- (hoare_asgn)
\{Q [X |-> a]\} X:=a \{Q\}

---------------------------------- (hoare_skip)
\{P\} SKIP \{P\}

\{P\} c1 \{Q\}
\{Q\} c2 \{R\}

---------------------------------- (hoare_seq)
\{P\} c1;;c2 \{R\}

\{P /\} c1 \{Q\}
\{P \b\} c2 \{Q\}

---------------------------------- (hoare_if)
\{P\} TEST b THEN c1 ELSE c2 FI \{Q\}

\{P \b\} c \{P\}

---------------------------------- (hoare_while)
\{P\} WHILE b DO c END \{P \b\}

\{P'\} c \{Q'\}
P \rightarrow P'
Q' \rightarrow Q

---------------------------------- (hoare_consequence)
\{P\} c \{Q\}
Decorated programs

(a) **SKIP** is locally consistent if its precondition and postcondition are the same:

\[ \{\{ P \}\} \textbf{SKIP} \{\{ P \}\} \]

(b) The sequential composition of \( c_1 \) and \( c_2 \) is locally consistent (with respect to assertions \( P \) and \( R \)) if \( c_1 \) is locally consistent (with respect to \( P \) and \( Q \)) and \( c_2 \) is locally consistent (with respect to \( Q \) and \( R \)):

\[ \{\{ P \}\} c_1 ; \; \{\{ Q \}\} c_2 \{\{ R \}\} \]

(c) An assignment is locally consistent if its precondition is the appropriate substitution of its postcondition:

\[ \{\{ P \} [X \rightarrow a] \}\} X := a \{\{ P \}\} \]

(d) A conditional is locally consistent (with respect to assertions \( P \) and \( Q \)) if the assertions at the top of its "then" and "else" branches are exactly \( P \land b \) and \( P \land \neg b \) and if its "then" branch is locally consistent (with respect to \( P \land b \) and \( Q \)) and its "else" branch is locally consistent (with respect to \( P \land \neg b \) and \( Q \)):

\[ \{\{ P \}\} \textbf{IF} b \textbf{THEN} \{\{ P \land b \}\}\} c_1 \{\{ Q \}\}\textbf{ELSE} \{\{ P \land \neg b \}\}\} c_2 \{\{ Q \}\}\textbf{FI} \{\{ Q \}\} \]

(e) A while loop with precondition \( P \) is locally consistent if its postcondition is \( P \land \neg b \) and if the pre- and postconditions of its body are exactly \( P \land b \) and \( P \):

\[ \{\{ P \}\} \textbf{WHILE} b \textbf{DO} \{\{ P \land b \}\}\} c_1 \{\{ P \}\}\textbf{END} \{\{ P \land \neg b \}\}\]

(f) A pair of assertions separated by \( \rightarrow \) is locally consistent if the first implies the second (in all states):

\[ \{\{ P \}\} \rightarrow \{\{ P' \}\} \]
Small-Step Imp

Arithmetic expressions:

Reserved Notation " t '/' st '-->a' t' "
(at level 40, st at level 39).

Inductive astep : state -> aexp -> aexp -> Prop :=
  | AS_Id : forall st i,
    AId i / st -->a ANum (st i)
  | AS_Plus1 : forall st a1 a1' a2, a1 / st -->a a1' ->
    (APlus a1 a2) / st -->a (APlus a1' a2)
  | AS_Plus2 : forall st v1 a2 a2',
    aval v1 ->
    a2 / st -->a a2' ->
    (APlus v1 a2) / st -->a (APlus v1 a2')
  | AS_Plus : forall st n1 n2,
    APlus (ANum n1) (ANum n2) / st -->a ANum (n1 + n2)
  | AS_Minus1 : forall st a1 a1' a2, a1 / st -->a a1' ->
    (AMinus a1 a2) / st -->a (AMinus a1' a2)
  | AS_Minus2 : forall st v1 a2 a2',
    aval v1 ->
    a2 / st -->a a2' ->
    (AMinus v1 a2) / st -->a (AMinus v1 a2')
  | AS_Minus : forall st n1 n2,
    (AMinus (ANum n1) (ANum n2)) / st -->a (ANum (minus n1 n2))
  | AS_Mult1 : forall st a1 a1' a2, a1 / st -->a a1' ->
    (AMult a1 a2) / st -->a (AMult a1' a2)
  | AS_Mult2 : forall st v1 a2 a2',
    aval v1 ->
    a2 / st -->a a2' ->
    (AMult v1 a2) / st -->a (AMult v1 a2')
  | AS_Mult : forall st n1 n2,
    (AMult (ANum n1) (ANum n2)) / st -->a (ANum (mult n1 n2))

where " t '/' st '-->a' t' " := (astep st t t').
Reserved Notation " t '/' st '->' t' '/' st' "
(at level 40, st at level 39, t' at level 39).

Open Scope imp_scope.

Inductive cstep : (com * state) -> (com * state) -> Prop :=
| CS_AssStep : forall st i a a',
  a / st --> a a' ->
  (i ::= a) / st --> (i ::= a') / st
| CS_Ass : forall st i n,
  (i ::= (ANum n)) / st --> SKIP / (i !-> n ; st)
| CS_SeqStep : forall st c1 c1' st' c2,
  c1 / st --> c1' / st' ->
  (c1 ;; c2) / st --> (c1' ;; c2) / st'
| CS_SeqFinish : forall st c2,
  (SKIP ;; c2) / st --> c2 / st
| CS_IfStep : forall st b b' c1 c2,
  b / st --> b b' ->
  TEST b THEN c1 ELSE c2 FI / st
  -->
  (TEST b' THEN c1 ELSE c2 FI) / st
| CS_IfTrue : forall st c1 c2,
  TEST BTrue THEN c1 ELSE c2 FI / st --> c1 / st
| CS_IfFalse : forall st c1 c2,
  TEST BFalse THEN c1 ELSE c2 FI / st --> c2 / st
| CS_While : forall st b c1,
  WHILE b DO c1 END / st
  -->
  (TEST b THEN c1 ;; WHILE b DO c1 END ELSE SKIP FI) / st

where " t '/' st '->' t' '/' st' " := (cstep (t, st) (t', st')).