CIS 500 — Software Foundations

Final Exam

(Standard and advanced versions together)

December 18, 2014

Answer key

(14 points)

1. **Properties of Imp Relations**

The propositions below concern basic properties of the Imp language. For each proposition, indicate whether it is true or false by circling either True or False. For reference, the definition of Imp, its evaluation semantics, and program equivalence (`cequiv`) starts on page 16.

(a) The evaluation relation for Imp is deterministic.

Answer: True

(b) The `cequiv` relation is symmetric.

Answer: True

(c) The command `WHILE BFalse DO SKIP END` is not equivalent to any other command.

Answer: False

(d) There is an Imp command `c` that terminates for some input states and diverges for others.

Answer: True

(e) If `cequiv c1 c2` then `cequiv (SKIP ;; c1) (SKIP ;; c2)`.

Answer: True

(f) For all arithmetic expressions `a1` and `a2`, we can show

```
cequiv   (X ::= a1 ;; Y ::= a2)  (Y ::= a2 ;; X ::= a1)
```

Answer: False

(g) If `SKIP / st || st'` then we know that `st` = `st'`.

Answer: True

(16 points)

2. **Hoare Logic**

The following Imp program (slowly) computes `X + Y`, placing the answer into `Z`.

```
Z ::= Y;;
WHILE X <> 0 DO
   Z ::= Z + 1;;
   X ::= X - 1
END
```

Below, add appropriate annotations in the provided spaces. You will need to give the outermost pre- and post-conditions; these assertions should show that the program works as described above. Use informal notations for mathematical formulae and assertions, but be completely precise 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 `->>`.

Mark the implication step(s) in your decoration (by circling the `->>`) that rely on the following fact. You may use other arithmetic facts silently.

- `forall a b c,  b <> 0 ->  (a + 1) + (b - 1) = a + b`

The Hoare rules and the rules for well-formed decorated programs are provided on pages 18 and 19.

```
{{ X = m  }}  ->>
{{ Y + X = m + Y }}
Z ::= Y
{{ Z + X = m + Y }}
WHILE X <> 0 DO
   {{ Z + X = m + Y /\ X <> 0 }} ->>
   {{ (Z + 1) + (X - 1) = m + Y }}
   Z ::= Z + 1;
   {{ Z + (X - 1) = m + Y }}
   X ::= X - 1
   {{ Z + X = m + Y }}
END
 {{ Z + X = m + Y /\ ~(X <> 0) }} ->>
 {{ Z = m + Y}}
```

Grading scheme:

- *1 point per each assignment back propagation*
- *1 point for including `X <> 0` and `(X <> 0)` at appropriate parts*
- *1 point for circling the correct implication*
- *4 points for specifying the program with an appropriate pre/post condition*

- *3 points for using an appropriate loop invariant*
- *4 points for propagating the loop invariant to the four places*

(20 points)

3. **Coq programming - Small-step semantics**

This problem refers to the Coq version of the small-step relation (`step`) for the Simply-typed Lambda Calculus with booleans, shown on page 22.

Because the `step` relation is deterministic, we can write a Coq function, called `next_step`, that computes what each term steps to (if any). The next page shows (part of) the definition of this function; you will need to complete the definition. Your implementation should satisfy the following correctness lemmas that state that `next_step` exactly corresponds to the `step` relation. (You do not need to prove these lemmas).

```
Lemma next_step_correct1 : forall t t' ,
       step t t' <-> next_step t = Some t'.
Lemma next_step_correct2 : forall t,
       normal_form step t <-> next_step t = None.
```

Below, the following example deminstrates the evaluation of the `next_step` function.

```
(* Identity function for booleans *)
Definition idB := tabs x TBool (tvar x).

Example ex0 : next_step (tapp idB ttrue) = Some ttrue.
```

(a) Fill in the blanks for the examples below. Some of these examples use `idB` defined above. Your answers should be consistent with the correctness lemmas.

```
Example ex1 : next_step ttrue = None.

Example ex2 : next_step (tapp ttrue tfalse) = None.

Example ex3 : next_step (tapp idB (tif ttrue tfalse ttrue)) =
  Some (tapp idB tfalse).

Example ex4 : next_step (tif ttrue (tapp idB ttrue) tfalse) =
  Some (tapp idB ttrue).
```

Grading scheme: 2 points per blank

(b) Now complete the *implementation* of the `next_step` function. The first few cases of this implementation have been given for you.

Your code may use the following helper function in your answer.

```
(* Determine whether the given term is a value *)
Fixpoint is_value (t : tm) : bool :=
  match t with
  | tabs x T u => true
  | ttrue      => true
  | tfalse     => true
  | _          => false
  end.

(* Calculate the next (small-)step for this term, if one exists *)
Fixpoint next_step (t : tm) : option tm :=
    match t with
    | tif ttrue t2 t3 => Some t2
    | tif tfalse t2 t3 => Some t3
    | tif t1 t2 t3 => match next_step t1 with
        | Some t1' =>  Some (tif t1' t2 t3)
        | None  => None
        end

    | tapp (tabs x T t1) t2 =>
        if is_value t2 then Some (subst x t2 t1)
        else match next_step t2 with
           | Some t2' => Some (tapp t1 t2')
           | None  => None
           end
    | tapp t1 t2 => match next_step t1 with
             | Some t1' => Some (tapp t1' t2)
             | None  => None
           end
    | _ => None
    end.
```

Grading scheme:

- *3 points for sending all values to None*
- *3 points for checking if t1 steps and return Some if so and None if t1 is not a value*
- *3 points for checking if t1 is a value and t2 steps and returning Some if so and None if t2 is not a value*
- *3 points for beta reduction when t1 and t2 are both values*
- *Various errors about pattern matching in Coq at discretion*

(14 points)

4. **Inductive Definitions and Scoping**

Consider the following Coq definitions for a simple language of expressions with constants, variables, and `options`.

```
Inductive tm : Type :=
| tnum   : nat -> tm                     (* Constants 0, 1, 2, ...    *)
| tvar   : id -> tm                      (* Variables X Y Z ...       *)
| tsome  : tm -> tm                      (* Some t1                   *)
| tnone  : tm                            (* None                      *)
| tmatch : tm -> tm -> id -> tm -> tm.   (* match t1 with
                                              | None   => t2
                                              | Some x => t3          *)
```

For example, we might encode the Coq expression

```
match x with
| None   => Some 0
| Some y => None
end
```

as

```
tmatch (tvar x) (tsome (tnum 0)) y tnone
```

The `tmatch` construct follows the usual variable scoping rules. That is, in the expression `tmatch t1 t2 X t3` the variable `X` is *bound* in `t3`.

Note that a variable `X` *appears free* in a term `t` if there is an occurrence of `X` that is not bound by a corresponding `tmatch`. Complete the following Coq definition of `afi` as an inductively defined relation such that `afi X t` is provable if and only if `X` appears free in `t`. You may use the next page if you need more space.

Answer:

```
Inductive afi : id -> tm -> Prop :=
| afi_var : forall x, afi x (tvar x)
| afi_some1 : forall x t1,
                afi x t1 ->
                afi x (tsome t1)
| afi_match1 : forall x y t1 t2 t3,
               afi x t1 ->
               afi x (tmatch t1 t2 y t3)
| afi_match2 : forall x y t1 t2 t3,
               afi x t2 ->
               afi x (tmatch t1 t2 y t3)
| afi_match3 : forall x y t1 t2 t3,
               x <> y ->
```

```
              afi x t3 ->
              afi x (tmatch t1 t2 y t3)
```
.

Grading scheme:

- *2 pts* - `afi_var`
- *2 pts* - `afi_some1`
- *2 pts* - `afi_match1`
- *2 pts* - `afi_match2`
- *4 pts* - `afi_match3`
- *2 pts* - *not having* `afi_none` *or* `afi_num` *(if other constructors are reasonable)*

(18 points)

5. **[Standard] Simply-typed Lambda Calculus**

This problem again considers the simply-typed lambda calculus with booleans. This language is type safe, a fact that can be proved using the standard preservation and progress proofs, and evaluation is deterministic.

Which of these properties are broken after each of the following modifications to STLC. (These modifications are made independently from one another.) In each case, circle each either "Remains true" or "Becomes false." For each one that becomes false, **give a counterexample**.

Grading scheme: 2 points per subcase

(a) Suppose that we add a new term `foo` with the following reduction rules:

```
--------------- (ST_Foo1)
(\x:A. x) ==> foo

--------------- (ST_Foo2)
foo ==> true
```

i. `step` is deterministic

Answer: Becomes false

ii. Progress

Answer: Remains true

iii. Preservation

Answer: Becomes false

Determinism fails because `(\x:Bool.x)true` steps to `foo true`. Preservation fails because `(\x:Bool.x)` steps to `foo`, which does not have a type.

(b) Suppose instead that we add the following new rule to the typing relation:

```
Γ ⊢ t1 ∈ Bool
Γ ⊢ t2 ∈ Bool
---------------------- (T_FunnyApp)
Γ ⊢ t1 t2 ∈ Bool
```

i. `step` is deterministic

Answer: Remains true

ii. Progress

Answer: Becomes false

iii. Preservation

Answer: Remains true

Progress breaks because `true false` doesn't step, but isn't a value.

(c) Suppose instead that we remove the rule `T_If` from the typing relation.

i. `step` is deterministic

Answer: Remains true

ii. Progress

Answer: Remains true

iii. Preservation

Answer: Remains true

(12 points)

6. **Subtyping**

The subtyping rules for STLC extended with pairs and records are given on page 25 for your reference. The subtyping relations among a collection of types can be visualized compactly in picture form: we draw a graph so that `S <: T` iff we can get from `S` to `T` by following arrows in the graph (either directly or indirectly). For example, a picture for the types `Top*Top`, `A*Top`, `Top*(Top*Top)`, and `Top*(A*A)` would look like this (it happens to form a tree, but that is not necessary in general):

$$\begin{tikzcd}
& \texttt{Top*Top} & \\
\texttt{A*Top} \arrow[ur] & & \texttt{Top*(Top*Top)} \arrow[ul] \\
& & \texttt{Top*(A*A)} \arrow[u]
\end{tikzcd}$$

Suppose we have defined types `A` and `B` so that `A <: B`. Draw a picture for the following eight types.

```
{}
{ m : A }
{ m : B }
{ k : B }
{ m : Top }
{ m : A , k : B }
Top
{ m : A } -> Top
```

Grading scheme: -2 points per mistake (i.e. arrow out of place). Answer:

$$\begin{tikzcd}
& & \texttt{Top} & \\
& \{\} \arrow[ur] & & \{\texttt{m} : \texttt{A}\} \to \texttt{Top} \arrow[ul] \\
\{\texttt{m} : \texttt{Top}\} \arrow[ur] & & \{\texttt{k} : \texttt{B}\} \arrow[ul] & \\
\{\texttt{m} : \texttt{B}\} \arrow[u] & & & \\
\{\texttt{m} : \texttt{A}\} \arrow[u] & & & \\
\{\texttt{m} : \texttt{A}, \texttt{k} : \texttt{B}\} \arrow[u] \arrow[uuurr] & & &
\end{tikzcd}$$

(16 points)

7. **[Standard] Subtyping**

   For each question, circle whether it is true or false. **Briefly justify your answer.**

   Grading scheme: 2 points for true/false, 2 points for justification

   (a) In STLC with subtyping (see the rules on page 24) there exists a type `T` such that `(\x:T. x x)` is typeable.

   Answer: True

   Why: `T = Top -> Top`

   (b) In STLC with subtyping, if we know $\Gamma \vdash$`\x:U.t` $\in$ `T`, then `T` must be equal to `U -> S` where Γ, `x : U` $\vdash$ `t` $\in$ `S`.

   Answer: False

   Why: Subsumption

   (c) In STLC with subtyping, if `A` is not equal to `Top`, then the type `A -> A` is a subtype of `Top -> A`.

   Answer: False

   Why: It is a supertype.

   (d) The *largest* type `U` that makes the assertion below true is `(A->A * B->B)`. (Recall that if `S <: T`, then we say that `T` is larger than `S`.)

   `empty` $\vdash$ `(\p:(A->A * B->B). p) ((\z:A.z), (\z:B.z))` $\in$ `U`

   Answer: False

   Why: False: that is the smallest type. The largest type is Top.

(18 points)

8. [**Advanced**] **Informal Proofs - Subtyping**

Give a detailed proof of the following inversion lemma for typing abstractions in STLC with subtyping (see the rules on page 24). You should prove this lemma for the with booleans and functions only, not the extension with product and record types.

Lemma (Typing Inversion for Abstractions): If $\Gamma \vdash$ `\x:S1.t2` $\in$ `T`, then there is a type `S2` such that Γ, `x:S1` $\vdash$ `t2` $\in$ `S2` and `S1 -> S2 <: T`.

Proof: Let `Gamma`, `x`, `S1`, `t2` and `T` be given as described. Proceed by induction on the derivation of `Γ` $\vdash$ `\x:S1.t2` $\in$ `T`. Cases `T_Var`, `T_App`, are vacuous as those rules cannot be used to give a type to a syntactic abstraction.

- If the last step of the derivation is a use of `T_Abs` then there is a type `T12` such that `T = S1 -> T12` and `Γ,x:S1` $\vdash$ `t2` $\in$ `T12`. Picking `T12` for `S2` gives us what we need: `S1 -> T12 <: S1 -> T12` follows from `S_Refl`.
- If the last step of the derivation is a use of `T_Sub` then there is a type `S` such that `S <: T` and `Γ` $\vdash$ `\x:S1.t2` $\in$ `S`. The IH for the typing subderivation tell us that there is some type `S2` with `S1 -> S2 <: S` and `Γ, x:S1`$\vdash$ `t2` $\in$ `S2`. Picking type `S2` gives us what we need, since `S1 -> S2 <: T` then follows by `S_Trans`.

Grading scheme:

- *2 points for proof by induction*
- *2 points for having a T_Abs case*
- *2 points for having a T_Sub case*
- *2 points for observing that other cases are trivial*
- *3 points for saying what is known about typing in T_Abs case*
- *2 points for saying what is known about typing in T_Sub case*
- *3 points for using IH*
- *2 points for using transitivity of subtyping*

Proofs attempts by inversion on the subtyping relation received very little credit.

(16 points)

9. [**Advanced**] **Informal Proofs — Progress with null**

In this problem we will extend STLC with `null`. Your job will be to state and prove a progress lemma for this extension. Although we will work with informal notation for this problem, the base language is the one specified by the Coq formalization, starting on page 21. In particular, there is no subtyping in this language.

Informally, the only change we will make to the syntax of the language is to add `null`,

```
t ::=  x
    |  \x:T .t
    |  t1 t2
    |  true
    |  false
    |  if t1 then t2 else t3
    |  null
```

which is a new form of value.

```
                ----------  (v_null)
                value null
```

We also add one new typing rule, shown below, that allows the `null` value to have any type.

```
                --------------- (T_Null)
                Γ ⊢ null ∈ T
```

(The call-by-value operational semantics for this language is unchanged.)

The standard progress lemma doesn't hold for STLC with this extension. The problem is that a term could get stuck when trying to use a `null` value. For example the term `if null then t1 else t2` is well typed, but isn't a value and doesn't step. We say that stuck terms like this one throw *null pointer exceptions*. In this problem, we won't model those exceptions directly. Instead, we define a relation, called `npe`, that describes where they should occur. We can use this relation to modify the Progress lemma (as shown on the next page) so that it is true.

The `npe` relation (shown on the next page) characterizes those terms that should throw null pointer exceptions. This relation includes terms that try to use `null` as another sort of value. It does not include any other stuck terms.

Your task for this problem is to complete the proof of this revised progress lemma.

Hint: This question is asking whether you understand the proof of the progress lemma for STLC. You will receive ***half*** *credit for recreating the appropriate parts of the standard proof here, without the extension to null.*

The `npe` relation

```
    ----------------------------------  NPE_If
      npe (if null then t1 else t2)

                npe t1
    ----------------------------------  NPE_If1
      npe (if t1 then t2 else t3)


                 npe t1
    ----------------------------------  NPE_App
              npe (null t1)


                npe t1
    ----------------------------------  NPE_App1
              npe (t1 t2)


          value t1     npe t2
    ----------------------------------  NPE_App2
              npe (t1 t2)
```

Lemma (Progress): For all `t` and `T`, if $\emptyset \vdash$ `t` $\in$ `T` then either `t` is a value, throws a null pointer exception, or steps. (i.e. either `value t` or `npe t` holds or there exists some `t'` such that `t ==> t'`).

Proof: by induction on the derivation of $\emptyset \vdash$ `t` $\in$ `T`.

- The last rule of the derivation cannot be `T_Var`, since a variable is never well typed in an empty context.
- The `T_Null`, `T_True`, `T_False`, and `T_Abs` cases are trivial, because in each of these cases we know immediately that `t` is a value.
- If the last rule of the derivation was `T_If`, then ... `t = if t1 then t2 else t3`, where `t1` has type `Bool`. By the IH, `t1` either is a value or takes a step or is a NPE.
  - Subcase: If `t1` is a value, then since it has type `Bool` it must be either `true` or `false` or `null`. If it is `true`, then `t` steps to `t2`; if false, it steps to `t3`, otherwise it is a NPE.
  - Subcase: Otherwise, if `t1` takes a step, and therefore so does `t` (by `ST_If`).
  - Subcase: Otherwise, if t1 is a NPE, then the if expression is a NPE.
- If the last rule of the derivation was `T_App`, then ... *Answer:* `t = t1 t2`, and we know that `t1` and `t2` are also well typed in the empty context; in particular, there exists a type `T2` such

that $\vdash$`t1` $\in$ `T2 -> T` and $\vdash$`t2` $\in$ `T2`. By the induction hypothesis, either `t1` is a value, or it can take an evaluation step, or `npe t1`.

- Subcase: If `t1` is a value, we now consider `t2`, which by the other induction hypothesis must also either be a value, take an evaluation step, or be a NPE.
    - Suppose `t2` is a value. Since `t1` is a value with an arrow type, it must either be a lambda abstraction or null; therefore either `t1 t2` can take a step by `ST_AppAbs`, or we have a NPE `null t2`.
    - Otherwise, if `t2` can take a step, then so can `t1 t2` by `ST_App2`.
    - Finally, if `t2` is a NPE then we are done by `NPE_App2`.
- Subcase: If `t1` can take a step, then so can `t1 t2` by `ST_App1`.
- Subcase: If `npe t1` then we are done by `NPE_App1`.

Grading scheme:

- *2 points for using IH for t1 to say there are 3 cases*
- *2 points for using IH for t2 to say there are 3 cases*
- *4 points for case where t1 is a value and t2 is a value (using inversion of typing to observe that t1 could be either lambda or null)*
- *2 points where t1 is a value and t2 steps*
- *2 points where t1 is a value and npe t2*
- *2 points where t1 steps*
- *2 points where t1 is a npe*

(`T_App` case of the revised progress proof).

Formal definitions for Imp

Syntax

```
Inductive aexp : Type :=
  | ANum : nat -> aexp
  | AId : id -> aexp
  | APlus : aexp -> aexp -> aexp
  | AMinus : aexp -> aexp -> aexp
  | AMult : aexp -> aexp -> aexp.

Inductive bexp : Type :=
  | BTrue : bexp
  | BFalse : bexp
  | BEq : aexp -> aexp -> bexp
  | BLe : aexp -> aexp -> bexp
  | BNot : bexp -> bexp
  | BAnd : bexp -> bexp -> bexp.

Inductive com : Type :=
  | CSkip : com
  | CAss : id -> aexp -> com
  | CSeq : com -> com -> com
  | CIf : bexp -> com -> com -> com
  | CWhile : bexp -> com -> com.

Notation "'SKIP'" :=
  CSkip.
Notation "l '::=' a" :=
  (CAss l a) (at level 60).
Notation "c1 ; c2" :=
  (CSeq c1 c2) (at level 80, right associativity).
Notation "'WHILE' b 'DO' c 'END'" :=
  (CWhile b c) (at level 80, right associativity).
Notation "'IFB' e1 'THEN' e2 'ELSE' e3 'FI'" :=
  (CIf e1 e2 e3) (at level 80, right associativity).
```

Evaluation relation

```
Inductive ceval : com -> state -> state -> Prop :=
  | E_Skip : forall st,
      SKIP / st || st
  | E_Ass  : forall st a1 n X,
      aeval st a1 = n ->
      (X ::= a1) / st || (update st X n)
  | E_Seq : forall c1 c2 st st' st'',
      c1 / st  || st' ->
      c2 / st' || st'' ->
      (c1 ; c2) / st || st''
  | E_IfTrue : forall st st' b1 c1 c2,
      beval st b1 = true ->
      c1 / st || st' ->
      (IFB b1 THEN c1 ELSE c2 FI) / st || st'
  | E_IfFalse : forall st st' b1 c1 c2,
      beval st b1 = false ->
      c2 / st || st' ->
      (IFB b1 THEN c1 ELSE c2 FI) / st || st'
  | E_WhileEnd : forall b1 st c1,
      beval st b1 = false ->
      (WHILE b1 DO c1 END) / st || st
  | E_WhileLoop : forall st st' st'' b1 c1,
      beval st b1 = true ->
      c1 / st || st' ->
      (WHILE b1 DO c1 END) / st' || st'' ->
      (WHILE b1 DO c1 END) / st || st''

  where "c1 '/' st '||' st'" := (ceval c1 st st').
```

Program equivalence

```
Definition bequiv (b1 b2 : bexp) : Prop :=
  forall (st:state), beval st b1 = beval st b2.

Definition cequiv (c1 c2 : com) : Prop :=
  forall (st st' : state),
    (c1 / st || st') <-> (c2 / st || st').
```

Hoare triples

```
Definition hoare_triple (P:Assertion) (c:com) (Q:Assertion) : Prop :=
  forall st st', c / st || st' -> P st  -> Q st'.

Notation "{{ P }} c {{ Q }}" := (hoare_triple P c Q).
```

Implication on assertions

```
Definition assert_implies (P Q : Assertion) : Prop :=
  forall st, P st -> Q st.

Notation "P ->> Q" := (assert_implies P Q) (at level 80).
```

(ASCII `->>` is typeset as a hollow arrow in the rules below.)

Hoare logic rules

$$\frac{}{\{\!\{\, \texttt{assn\_sub X a } Q \,\}\!\}\ \texttt{X := a}\ \{\!\{\, Q \,\}\!\}}\quad (\texttt{hoare\_asgn})$$

$$\frac{}{\{\!\{\, P \,\}\!\}\ \texttt{SKIP}\ \{\!\{\, P \,\}\!\}}\quad (\texttt{hoare\_skip})$$

$$\frac{\begin{array}{c}\{\!\{\, P \,\}\!\}\ \texttt{c1}\ \{\!\{\, Q \,\}\!\} \\ \{\!\{\, Q \,\}\!\}\ \texttt{c2}\ \{\!\{\, R \,\}\!\}\end{array}}{\{\!\{\, P \,\}\!\}\ \texttt{c1; c2}\ \{\!\{\, R \,\}\!\}}\quad (\texttt{hoare\_seq})$$

$$\frac{\begin{array}{c}\{\!\{\, P \wedge b \,\}\!\}\ \texttt{c1}\ \{\!\{\, Q \,\}\!\} \\ \{\!\{\, P \wedge \sim b \,\}\!\}\ \texttt{c2}\ \{\!\{\, Q \,\}\!\}\end{array}}{\{\!\{\, P \,\}\!\}\ \texttt{IFB b THEN c1 ELSE c2 FI}\ \{\!\{\, Q \,\}\!\}}\quad (\texttt{hoare\_if})$$

$$\frac{\{\!\{\, P \wedge b \,\}\!\}\ \texttt{c}\ \{\!\{\, P \,\}\!\}}{\{\!\{\, P \,\}\!\}\ \texttt{WHILE b DO c END}\ \{\!\{\, P \wedge \sim b \,\}\!\}}\quad (\texttt{hoare\_while})$$

$$\frac{\begin{array}{c}\{\!\{\, P' \,\}\!\}\ \texttt{c}\ \{\!\{\, Q' \,\}\!\} \\ P \rightarrowtriangle P' \\ Q' \rightarrowtriangle Q\end{array}}{\{\!\{\, P \,\}\!\}\ \texttt{c}\ \{\!\{\, Q \,\}\!\}}\quad (\texttt{hoare\_consequence})$$

$$\frac{\begin{array}{c}\{\!\{\, P' \,\}\!\}\ \texttt{c}\ \{\!\{\, Q \,\}\!\} \\ P \rightarrowtriangle P'\end{array}}{\{\!\{\, P \,\}\!\}\ \texttt{c}\ \{\!\{\, Q \,\}\!\}}\quad (\texttt{hoare\_consequence\_pre})$$

$$\frac{\begin{array}{c}\{\!\{\, P \,\}\!\}\ \texttt{c}\ \{\!\{\, Q' \,\}\!\} \\ Q' \rightarrowtriangle Q\end{array}}{\{\!\{\, P \,\}\!\}\ \texttt{c}\ \{\!\{\, Q \,\}\!\}}\quad (\texttt{hoare\_consequence\_post})$$

Decorated programs

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

```
{{ P }}
SKIP
{{ P }}
```

(b) The sequential composition of `c1` and `c2` is locally consistent (with respect to assertions `P` and `R`) if `c1` is locally consistent (with respect to `P` and `Q`) and `c2` is locally consistent (with respect to `Q` and `R`):

```
{{ P }}
c1;
{{ Q }}
c2
{{ R }}
```

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

```
{{ P [X |-> 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 /\ b` and `P /\ ~b` and if its "then" branch is locally consistent (with respect to `P /\ b` and `Q`) and its "else" branch is locally consistent (with respect to `P /\ ~b` and `Q`):

```
{{ P }}
IFB b THEN
  {{ P /\ b }}
  c1
  {{ Q }}
ELSE
  {{ P /\ ~b }}
  c2
  {{ Q }}
FI
{{ Q }}
```

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

```
{{ P }}
WHILE b DO
  {{ P /\ b }}
  c1
  {{ P }}
END
{{ P /\ ~b }}
```

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

```
{{ P }} ->>
{{ P' }}
```

Coq formalization of STLC with booleans

Identifiers

```
Inductive id : Type :=
  Id : nat -> id.

Theorem eq_id_dec : forall id1 id2 : id, {id1 = id2} + {id1 <> id2}.

Definition x := (Id 0).
Definition y := (Id 1).
Definition z := (Id 2).
```

Types

```
Inductive ty : Type :=
  | TBool  : ty
  | TArrow : ty -> ty -> ty.
```

Terms

```
Inductive tm : Type :=
  | tvar   : id -> tm
  | tapp   : tm -> tm -> tm
  | tabs   : id -> ty -> tm -> tm
  | ttrue  : tm
  | tfalse : tm
  | tif    : tm -> tm -> tm -> tm.

Inductive value : tm -> Prop :=
  | v_abs : forall x T t,
      value (tabs x T t)
  | v_true :
      value ttrue
  | v_false :
      value tfalse.
```

Substitution

```
Reserved Notation "'[' x ':=' s ']' t" (at level 20).

Fixpoint subst (x:id) (s:tm) (t:tm) : tm :=
  match t with
  | tvar x' =>
      if eq_id_dec x x' then s else t
  | tabs x' T t1 =>
      tabs x' T (if eq_id_dec x x' then t1 else ([x:=s] t1))
  | tapp t1 t2 =>
      tapp ([x:=s] t1) ([x:=s] t2)
  | ttrue =>
      ttrue
  | tfalse =>
      tfalse
  | tif t1 t2 t3 =>
      tif ([x:=s] t1) ([x:=s] t2) ([x:=s] t3)
  end

where "'[' x ':=' s ']' t" := (subst x s t).
```

Reduction

```
Reserved Notation "t1 '==>' t2" (at level 40).

Inductive step : tm -> tm -> Prop :=
  | ST_AppAbs : forall x T t12 v2,
         value v2 ->
         (tapp (tabs x T t12) v2) ==> [x:=v2]t12
  | ST_App1 : forall t1 t1' t2,
         t1 ==> t1' ->
         tapp t1 t2 ==> tapp t1' t2
  | ST_App2 : forall v1 t2 t2',
         value v1 ->
         t2 ==> t2' ->
         tapp v1 t2 ==> tapp v1  t2'
  | ST_IfTrue : forall t1 t2,
      (tif ttrue t1 t2) ==> t1
  | ST_IfFalse : forall t1 t2,
      (tif tfalse t1 t2) ==> t2
  | ST_If : forall t1 t1' t2 t3,
      t1 ==> t1' ->
      (tif t1 t2 t3) ==> (tif t1' t2 t3)

where "t1 '==>' t2" := (step t1 t2).

Definition normal_form {X:Type} (R:relation X) (t:X) : Prop :=
  ~ exists t', R t t'.
```

Contexts

```
Definition partial_map (A:Type) := id -> option A.

Definition empty {A:Type} : partial_map A := (fun _ => None).
Definition extend {A:Type} (Gamma : partial_map A) (x:id) (T : A) :=
  fun x' => if eq_id_dec x x' then Some T else Gamma x'.
```

Typing Relation

```
Reserved Notation "Gamma '|-' t '\in' T" (at level 40).

Inductive has_type : context -> tm -> ty -> Prop :=
  | T_Var : forall Gamma x T,
      Gamma x = Some T ->
      Gamma |- tvar x \in T
  | T_Abs : forall Gamma x T11 T12 t12,
      extend Gamma x T11 |- t12 \in T12 ->
      Gamma |- tabs x T11 t12 \in TArrow T11 T12
  | T_App : forall T11 T12 Gamma t1 t2,
      Gamma |- t1 \in TArrow T11 T12 ->
      Gamma |- t2 \in T11 ->
      Gamma |- tapp t1 t2 \in T12
  | T_True : forall Gamma,
       Gamma |- ttrue \in TBool
  | T_False : forall Gamma,
       Gamma |- tfalse \in TBool
  | T_If : forall t1 t2 t3 T Gamma,
       Gamma |- t1 \in TBool ->
       Gamma |- t2 \in T ->
       Gamma |- t3 \in T ->
       Gamma |- tif t1 t2 t3 \in T

where "Gamma '|-' t '\in' T" := (has_type Gamma t T).
```

STLC with subtyping

Typing relation

```
                           Γ x = T
                          --------------                              (T_Var)
                          Γ ⊢ x ∈ T

                   Γ, x:T11 ⊢ t12 ∈ T12
                  ----------------------------                        (T_Abs)
                  Γ ⊢ \x:T11.t12 ∈ T11->T12

                     Γ ⊢ t1 ∈ T11->T12
                       Γ ⊢ t2 ∈ T11
                     ----------------------                           (T_App)
                      Γ ⊢ t1 t2 ∈ T12

                      --------------------                           (T_True)
                      Γ ⊢ true ∈ Bool

                     ---------------------                          (T_False)
                     Γ ⊢ false ∈ Bool

   Γ ⊢ t1 ∈ Bool    Γ ⊢ t2 ∈ T    Γ ⊢ t3 ∈ T
   --------------------------------------------------------            (T_If)
            Γ ⊢ if t1 then t2 else t3 ∈ T

                    G ⊢ t ∈ S     S <: T
                  -------------------------                       (T_Sub)
                        Γ ⊢ t ∈ T
```

Subtyping relation

```
                      S <: U    U <: T
                      ----------------                       (S_Trans)
                           S <: T

                           ------                             (S_Refl)
                           T <: T

                           --------                            (S_Top)
                           S <: Top

                    T1 <: S1    S2 <: T2
                    --------------------                     (S_Arrow)
                      S1->S2 <: T1->T2
```

STLC subtyping, extended with pairs and records

Subtyping relation

```
                   S1 <: T1    S2 <: T2
                   --------------------                    (S_Prod)
                      S1*S2 <: T1*T2


                          n > m
             ---------------------------------              (S_RcdWidth)
             {i1:T1...in:Tn} <: {i1:T1...im:Tm}


                   S1 <: T1  ...  Sn <: Tn
              ----------------------------------            (S_RcdDepth)
              {i1:S1...in:Sn} <: {i1:T1...in:Tn}


     {i1:S1...in:Sn} is a permutation of {i1:T1...in:Tn}
     ---------------------------------------------------        (S_RcdPerm)
              {i1:S1...in:Sn} <: {i1:T1...in:Tn}
```