CIS 500 — Software Foundations

Final Exam

(Standard and advanced versions together)

December 13, 2013

Answer key
1. (12 points) Multiple Choice — Coq Programming
   Circle the correct answer. (Each question has one unique correct answer.)

(a) What is the type of the Coq term: \((\text{fun } n: \text{nat} \Rightarrow n = 0)\)?
   i. nat \(\Rightarrow\) nat
   ii. Prop
   iii. nat \(\Rightarrow\) Prop \(\leftarrow this\ one\)
   iv. forall n:nat, n = 0
   v. ill typed

(b) What is the type of the Coq term: \((\forall n: \text{nat}, n = 0)\)?
   i. nat \(\Rightarrow\) nat
   ii. Prop \(\leftarrow this\ one\)
   iii. nat \(\Rightarrow\) Prop
   iv. forall n:nat, n = 0
   v. ill typed

(c) What is the type of the Coq term: \((\text{fun } (P: \text{nat} \Rightarrow \text{Prop}) (n: \text{nat}) (Q: P n) \Rightarrow Q)\)?
   i. nat \(\Rightarrow\) Prop \(\Rightarrow\) nat \(\Rightarrow\) Prop \(\Rightarrow\) Prop
   ii. forall (P : nat \(\Rightarrow\) Prop), nat \(\Rightarrow\) Prop
   iii. (nat \(\Rightarrow\) Prop) \(\Rightarrow\) (n:nat \(\Rightarrow\) P n) \(\Rightarrow\) Q
   iv. forall (P : nat \(\Rightarrow\) Prop) (n : nat), P n \(\Rightarrow\) P n \(\leftarrow this\ one\)
   v. ill typed

(d) What is the type of the Coq term: \(((\text{fun } P: \text{Prop} \Rightarrow P) (3 = 4))\)
   i. Prop \(\leftarrow this\ one\)
   ii. nat
   iii. nat \(\Rightarrow\) Prop
   iv. Prop \(\Rightarrow\) nat
   v. ill typed
2. (16 points) Multiple Choice — Imp Equivalence

Circle all correct answers. There may be zero or more than one. For reference, the definition of Imp, its evaluation semantics, and program equivalence (cequiv) start on page 17.

(a) Consider the Imp program:

```
IF X > 0 THEN
    WHILE X > 0 DO SKIP END
ELSE
    SKIP
FI
```

Which of the following are equivalent to it, according to cequiv?

i. WHILE X > 0 DO ii. SKIP iii. X ::= 0 iv. IF X > 1 THEN
    SKIP
    END

Answer: i, iv

(b) Consider the Imp program:

```
X ::= 0;;
Y ::= X + 1;;
```

Which of the following are equivalent to it, according to cequiv?

i. Y ::= 1;; ii. Y ::= 0;; iii. Y ::= 1;;
   WHILE X <> 0 DO X ::= X - X;;
   X ::= X - 1 Y ::= Y - 1;;
   END

Answer: i, iii, iv

(c) Consider an arbitrary Imp command c. Which of the following are equivalent to c, according to cequiv?

i. c ;; c ii. X ::= 1;; iii. IF X > 0 THEN
   WHILE X > 0 DO c SKIP
   c ;; X ::= X - 1 ELSE SKIP FI
   DONE

Answer: iv

(d) Which of the following propositions are provable?

i. forall c, (exists st:state, c / st || st) -> cequiv c SKIP
ii. \[\forall c_1 c_2 s_1 s_3,\]
\[((c_1 ;; c_2) / s_1 || s_3) \rightarrow (\exists s_2: \text{state}, c_1 / s_1 || s_2 /\ c_2 / s_2 || s_3).\]

iii. \[\forall c_1 c_2, \ (\text{cequiv} \ c_1 c_2) \rightarrow (\text{cequiv} \ (c_1;;c_2) \ (c_2;;c_1))\]

iv. \[\forall c, \ (\forall s, c / s || s) \rightarrow \text{cequiv} \ c \ \text{SKIP}.\]

\textit{Answer:} ii, iii, iv
3. (16 points) Hoare Logic

The following Imp program computes $m \times n$, placing the answer into $Z$.

\[
\begin{align*}
\text{\{\{ True \}\}} & \quad X ::= 0 ;; \\
\text{\{\{ Z = 0 \}\}} & \quad Z ::= 0 ;; \\
\text{WHILE } X \not= n \text{ DO} & \quad Y ::= 0 ;; \\
& \quad \text{WHILE } Y \not= m \text{ DO} \\
& \quad \quad Z ::= Z + 1 ;; \\
& \quad \quad Y ::= Y + 1 ;; \\
& \quad \text{END} \\
& \quad X ::= X + 1 ;; \\
\text{END} & \quad \{\{ Z = m \times n \}\}
\end{align*}
\]

On the next page, 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. Use informal notations for mathematical formulae and assertions, but please be completely precise and pedantic in the way you apply the Hoare rules — i.e., write out assertions in \textit{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 Hoare rules and the rules for well-formed decorated programs are provided on pages 19 and 20, for reference.
Mark the implication step(s) in your decoration (by circling the $\rightarrow\rightarrow$) that rely on the following fact. You may use other arithmetic facts silently.

- $m \cdot a + m = m \cdot (a + 1)$

\[
\begin{align*}
\{\{ \text{True } \}\} & \rightarrow\rightarrow \\
\{\{ 0 = m \cdot 0 \}\} & \\
X & ::= 0 \\
\{\{ 0 = m \cdot X \}\} & ;; \\
Z & ::= 0 \\
\{\{ Z = m \cdot X \}\} & ;; \\
\text{WHILE } X \not< n \text{ DO} & \\
\{\{ Z = m \cdot X \land X \not< n \}\} & \rightarrow\rightarrow \\
\{\{ Z = m \cdot X + 0 \}\} & \\
Y & ::= 0 \\
\{\{ Z = m \cdot X + Y \}\} & ;; \\
\text{WHILE } Y \not< m \text{ DO} & \\
\{\{ Z = m \cdot X + Y \land Y \not< m \}\} & \rightarrow\rightarrow \\
\{\{ (Z + 1) = m \cdot X + Y + 1 \}\} & \\
Z & ::= Z + 1 \\
\{\{ Z = m \cdot X + Y + 1 \}\} & ;; \\
Y & ::= Y + 1 \\
\{\{ Z = m \cdot X + Y \}\} & \\
\text{END} & \\
\{\{ Z = m \cdot X + Y \land \neg(Y \not< m) \}\} & \rightarrow\rightarrow \quad (* \text{THIS STEP} *) \\
\{\{ Z = m \cdot (X + 1) \}\};; \\
X & ::= X + 1 \\
\{\{ Z = m \cdot \text{st } X \}\} & \\
\text{END} & \\
\{\{ Z = m \cdot X \land \neg(X \not< n) \}\} & \rightarrow\rightarrow \\
\{\{ Z = m \cdot n \}\} & \\
\end{align*}
\]

Grading scheme:

- 1 point per implication
- 1 point for circling the correct implication
- 4 points for correct “back propagation” of the mechanical parts of the annotation process
- 3 points for each loop invariant
4. (16 points) Inductive Definitions and Scoping

Consider the following Coq definitions for a simple language of arithmetic expressions with constants, variables, plus, and let.

Definition id := nat.
Inductive tm : Type :=
| tnum : nat -> tm (* Constants 0, 1, 2, ... *)
| tvar : id -> tm (* Variables X Y Z ... *)
| tplus : tm -> tm -> tm (* Plus: t1 + t2 *)
| tlet : id -> tm -> tm -> tm (* Let: let X = t1 in t2 *)

The let construct follows the usual variable scoping rules. That is, in let X = t1 in t2, written in Coq as (tlet X t1 t2), the variable X is bound in t2.

Recall that a variable X appears free in a term t if there is an occurrence of X that is not bound by a corresponding let. 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.

Answer:

Inductive afi : id -> tm -> Prop :=
| afi_var : forall x, afi x (tvar x)
| afi_plus1 : forall x t1 t2, afi x t1 -> afi x (tplus t1 t2)
| afi_plus2 : forall x t1 t2, afi x t2 -> afi x (tplus t1 t2)
| afi_let1 : forall x y t1 t2, afi x t1 -> afi x (tlet y t1 t2)
| afi_let2 : forall x y t1 t2, x <> y -> afi x t2 -> afi x (tlet y t1 t2)
5. [Advanced] (20 points) Informal Proofs — Substitution

Your job in this problem is to prove a substitution lemma. First, we extend the let language from the previous problem by adding a unit constant. Informally, the grammar of the terms and types for the resulting language is given by:

\[
\begin{align*}
t & ::= (* \text{ Terms } *) \\
& \mid () \quad (* \text{ Unit constant } *) \\
& \mid n \quad (* \text{ Natural numbers } *) \\
& \mid X \quad (* \text{ Variables } *) \\
& \mid t + t \quad (* \text{ Sum } *) \\
& \mid \text{let } X = t \text{ in } t \quad (* \text{ Let } *)
\end{align*}
\]

\[
\begin{align*}
T & ::= (* \text{ Types } *) \\
& \mid \text{Unit} \\
& \mid \text{Nat} \\
& \mid \text{Variables} \\
& \mid t + t \\
& \mid \text{let } X = t \text{ in } t
\end{align*}
\]

The type system is given by:

\[
\begin{align*}
\Gamma & \vdash X \in T \\
\Gamma & \vdash n \in \text{Nat} \\
\Gamma & \vdash () \in \text{Unit}
\end{align*}
\]

\[
\begin{align*}
\Gamma & \vdash t_1 \in \text{Nat} \quad \Gamma \vdash t_2 \in \text{Nat} \quad \Gamma, X:T \vdash t_2 \in T_2 \\
\Gamma & \vdash t_1 \in T_1 \\
\Gamma & \vdash \text{let } X = t_1 \text{ in } t_2 \in T_2
\end{align*}
\]

The substitution operation is defined by:

\[
\begin{align*}
[X:=s]() &= () \\
[X:=s]n &= n \\
[X:=s]X &= s \\
[X:=s]Y &= Y \quad \text{(if } X \neq Y) \\
[X:=s](t_1 + t_2) &= ([X:=s]t_1 + [X:=s]t_2) \\
[X:=s](\text{let } X = t_1 \text{ in } t_2) &= (\text{let } X = [X:=s]t_1 \text{ in } t_2) \\
[X:=s](\text{let } Y = t_1 \text{ in } t_2) &= (\text{let } Y = [X:=s]t_1 \text{ in } [X:=s]t_2) \quad \text{(if } x \neq Y)
\end{align*}
\]

Also recall the following lemma, which makes use of the concept of “appears free in” from the previous problem. You do not need to prove this lemma.

**Lemma:** Context Invariance

Suppose \( \Gamma \vdash t \in T \) and that, for all \( X \), if \( X \) appears free in \( t \) then \( \Gamma' X = \Gamma X \). Then \( \Gamma' \vdash t \in T \).
Give a careful, informal proof of the substitution lemma for this language. You may freely use functional extensionality to reason about context equivalence, and you may find it helpful to invoke the context invariance lemma at some point(s).

**Lemma:** Substitution Preserves Typing

For all \( t, v, X, \Gamma, T, \text{ and } U \), if \( \Gamma, X:U \vdash t \in T \) and \( \vdash v \in U \) then \( \Gamma \vdash [X:=v]t \in T \).

**Proof:** By induction on the structure of \( t \); importantly the induction hypothesis generalizes over \( \Gamma \) and \( T \). There are five cases to consider:

- **Case:** \( t = () \). By inversion on the typing relation we have that \( T = \text{Unit} \) and, by the definition of substitution, we have \( [X:=v]() = () \). It remains to show that \( \Gamma \vdash () \in \text{Unit} \), but this follows immediately from rule \( \text{T_Unit} \).

- **Case:** \( t = n \). This case is similar to the case above.

- **Case:** \( t = Y \) for some variable \( Y \). There are two subcases to consider.
  - **Subcase:** \( X = Y \). Then, by inversion of the typing relation we have that \( T = U \) and, by the definition of substitution, we have \( [X:=v]X = v \). It remains to show that \( \Gamma \vdash v \in T \), but, since \( T=U \), and \( v \) is closed, the result follows by context invariance.
  - **Subcase:** \( X <> Y \). Then, by inversion of the typing relation, we have that \( (\Gamma, X:U)Y = T \) and, by the definition of substitution, we have \( [X:=v]Y = Y \). It remains to show that \( \Gamma \vdash Y \in T \), but this follows from \( \text{T_Var} \) because, since \( X <> Y \), we have \( T = (\Gamma, X:U)Y = \Gamma Y \).

- **Case:** \( t = t_1 + t_2 \). Then, by inversion of the typing relation, we have \( T = \text{Nat} \) and both \( \Gamma, X:U \vdash t_1 \in \text{Nat} \) and \( \Gamma, X:U \vdash t_2 \in \text{Nat} \). By two applications of the induction hypothesis, we obtain \( \Gamma \vdash [X:=v]t_1 \in \text{Nat} \) and \( \Gamma \vdash [X:=v]t_2 \in \text{Nat} \). The result follows directly via the \( \text{T_Sum} \) rule.

- **Case:** \( t = \text{let } Y = t_1 \text{ in } t_2 \). By inversion of the typing relation, we have that \( T = T_2 \) and both \( \Gamma, X:U \vdash t_1 \in T_1 \) and \( \Gamma, X:U, Y:T_1 \vdash t_2 \in T_2 \). By the induction hypothesis applied to the first of these, we know that \( \Gamma \vdash [X:=v]t_1 \in T_1 \); call this fact (*) . There are two subcases to consider.
  - **Subcase:** \( X = Y \). Then, by the definition of substitution, it suffices to show that we have \( \Gamma \vdash \text{let } X = [X:=v]t_1 \text{ in } t_2 \in T_2 \). Note that, by function extensionality, we have that \( \Gamma, X:U, X:T_1 = \Gamma, X:T_1 \), and so we also have \( \Gamma, X:T_1 \vdash t_2 \in T_2 \). The conclusion then follows directly from this fact and (*) by using the \( \text{T_Let} \) rule.
  - **Subcase:** \( X <> Y \). Then, by the definition of substitution, it suffices to show that we have \( \Gamma \vdash \text{let } X = [X:=v]t_1 \text{ in } [X:=v]t_2 \in T_2 \). Note that, by functional extensionality and \( X <> Y \) we have \( (\Gamma, X:U, Y:T_1) = (\Gamma, Y:T_1, X:U) \). By a second use of the induction hypothesis instantiated with the context \( \Gamma, Y:T_1 \), we find that \( \Gamma, Y:T_1 \vdash [X:=v]t_2 \in T_2 \). The conclusion follows immediately from this fact and (*) using the \( \text{T_Let} \) rule.
6. **[Standard]** (12 points) Multiple Choice — Simply-typed Lambda Calculus

Mark all correct answers. There may be zero or more than one.

In this problem we consider a variant of the simply-typed lambda calculus with natural numbers, the syntax, small-step semantics, and typing rules for which are given starting on page 22. Note: for this problem we do not consider STLC with subtyping, fix, or other extensions.

This language is type safe, a fact that can be proved using the standard preservation, and progress proofs, and evaluation is deterministic.

(a) Which of the following properties would still hold if we remove the predicate `value v1` from the ST_App2 rule?

i. step is deterministic

ii. Progress ← this one

iii. Preservation ← this one

(b) Which of the following properties would still hold if we add the following rule to the step relation?

\[(0, 0) \Rightarrow 0\]

i. step is deterministic ← this one

ii. Progress ← this one

iii. Preservation ← this one

(c) Which of the following properties would still hold if we replace the T_App rule with the following variant?

\[
\Gamma \vdash t_1 \in \text{Nat} \rightarrow T_{12} \\
\Gamma \vdash t_2 \in \text{Nat} \\
\text{-----------------------} \\
\Gamma \vdash t_1 t_2 \in T_{12}
\]

i. step is deterministic ← this one

ii. Progress ← this one

iii. Preservation ← this one

(d) Which of the following properties would still hold if we added the following typing rule?

\[
\Gamma \vdash t_1 \in \text{Nat} \\
\Gamma \vdash t_2 \in \text{Nat} \\
\text{-----------------------} \\
\Gamma \vdash t_1 t_2 \in \text{Nat}
\]

i. step is deterministic ← this one

ii. Progress

iii. Preservation ← this one
In this problem we will develop a variant of the simply-typed lambda calculus with natural numbers and an induction operator. The starting point is the plain simply typed lambda with a base type of natural numbers and constructors for the constant zero 0 and successor S.

You can find the syntax, typing rules, and small-step evaluation rules for this part of the language beginning on page 22. Note: for this problem we do not consider STLC with subtyping, fix, or other extensions.

(a) Recall that we can draw typing derivations as “trees” where each node is a judgment of the form \( \Gamma \vdash t \in T \). The root of the tree (pictured at the bottom of the drawing) is the desired conclusion, and each premise is a subtree that instantiates a typing rule. For example, the following is a legal typing derivation:

\[
\begin{align*}
\text{T_Zero} & \quad \Gamma \vdash 0 \in \text{Nat} \\
\text{T_Succ} & \quad \Gamma \vdash S\ 0 \in \text{Nat} \\
\text{T_Abs} & \quad \vdash \lambda x: \text{Nat}. (S\ 0) \in \text{Nat} \rightarrow \text{Nat}
\end{align*}
\]

Complete the typing derivation given below. Label the inference rule used at each node of the tree. Note that the type of the root judgment needs to be filled in.

\[
\begin{align*}
\text{T_Var} & \quad \Gamma \vdash x \in \text{Nat} \\
\text{T_Var} & \quad \Gamma \vdash y \in \text{Nat} \rightarrow \text{Nat} \\
\text{T_Succ} & \quad \Gamma \vdash S\ x \in \text{Nat} \\
\text{T_App} & \quad \Gamma \vdash y\ (S\ x) \in \text{Nat} \\
\text{T_Succ} & \quad \Gamma \vdash S\ (y\ (S\ x)) \in \text{Nat} \\
\text{T_Abs} & \quad \Gamma \vdash \lambda y: \text{Nat} \rightarrow \text{Nat}.\ S\ (y\ (S\ x)) \in \text{Nat} \rightarrow \text{Nat} \\
\end{align*}
\]
Rather than adding if0 and the general recursion operator fix, here we follow Coq and add a built-in form of natural-number induction.

\[ t ::= \ldots \]
\[ | \text{nat\_ind } t \ t \ t \]

The term \text{nat\_ind } tz ts tn acts like a fold over the natural number datatype. The term tz specifies what to do for the base (zero) case of the induction, and the term ts (successor) shows how to compute the answer for S n given n itself and the inductive result for n. The argument tn is the natural number over which induction is being done.

Once we have added nat\_ind to the STLC, we can write many familiar programs using natural numbers. For example, here is a function that adds two natural numbers, defined by induction on n. The base case is just m and the inductive step computes the successor of the recursive result:

\[
(* \text{Nat\_plus } *) \quad \forall n:\text{Nat}. \forall m:\text{Nat}. \text{nat\_ind } m (\forall x:\text{Nat}. \forall y:\text{Nat}. S y) n
\]

The steps it takes when computing Nat\_plus 2 1 look like this, where we have marked the novel behavior of nat\_ind with !!:

\[
(\forall n:\text{Nat}. \forall m:\text{Nat}. \text{nat\_ind } m (\forall x:\text{Nat}. \forall y:\text{Nat}. S y) n) (S S 0) (S 0)
\Rightarrow
\]
\[
(\forall m:\text{Nat}. \text{nat\_ind } m (\forall x:\text{Nat}. \forall y:\text{Nat}. S y) (S S 0)) (S 0)
\Rightarrow
\]
\[
\text{nat\_ind } (S 0) (\forall x:\text{Nat}. \forall y:\text{Nat}. S y) (S S 0)
\Rightarrowarena{inductive case}
\]
\[
(\forall x:\text{Nat}. \forall y:\text{Nat}. S y) (S 0) (\text{nat\_ind } (S 0) (\forall x:\text{Nat}. \forall y:\text{Nat}. S y) (S 0))
\Rightarrowarena{inductive case}
\]
\[
(\forall x:\text{Nat}. \forall y:\text{Nat}. S y) (S 0) ((\forall x:\text{Nat}. \forall y:\text{Nat}. S y) 0 (\text{nat\_ind } (S 0) (\forall x:\text{Nat}. \forall y:\text{Nat}. S y) 0))
\Rightarrowarena{base case}
\]
\[
(\forall x:\text{Nat}. \forall y:\text{Nat}. S y) (S 0) ((\forall x:\text{Nat}. \forall y:\text{Nat}. S y) 0 (S 0))
\Rightarrow
\]
\[
(\forall x:\text{Nat}. \forall y:\text{Nat}. S y) (S 0) ((\forall y:\text{Nat}. S y) (S 0))
\Rightarrow
\]
\[
(\forall x:\text{Nat}. \forall y:\text{Nat}. S y) (S 0) (S (S 0))
\Rightarrow
\]
\[
(\forall y:\text{Nat}. S y) (S (S 0))
\Rightarrow
\]
\[
S (S (S 0))
\]

In general, the small step semantics of nat\_ind should work like:

\[ \text{nat\_ind } vz \ vs \ 3 \implies* \ vs \ 2 \ (vs \ 1 \ (vs \ 0 \ vz)) \]

where we write 3 as a shorthand for S S S 0, etc.
Define the small-step operational semantics for \texttt{nat\_ind}. There are three “structural” rules that evaluate the arguments to \texttt{nat\_ind} in order from left-to-right. The first such rule is:

\[
\begin{align*}
tz & \implies tz' \\
\text{-----------------------------} \\
\text{nat\_ind tz ts tn} & \implies \text{nat\_ind tz' ts tn}
\end{align*}
\]

Write the other two structural rules below. Use the \texttt{value} predicate as appropriate.

\[
\begin{align*}
\text{value vz ts} & \implies ts' \\
\text{-----------------------------} \\
\text{nat\_ind vz ts tn} & \implies \text{nat\_ind vz ts' tn}
\end{align*}
\]

\[
\begin{align*}
\text{value vz tn} & \implies tn' \quad \text{value vs} \\
\text{-----------------------------} \\
\text{nat\_ind vz vs tn} & \implies \text{nat\_ind vz vs tn'}
\end{align*}
\]

After reducing all three arguments to values, the “interesting” rules of the small step semantics do case analysis on the third argument, yielding the base case, or performing a recursive call as appropriate. Complete these two rules for the small-step operational semantics of \texttt{nat\_ind}.

\[
\begin{align*}
\text{value vz value vs} & \\
\text{-----------------------------} \\
\text{nat\_ind vz vs 0} & \implies vz \\
\text{nat\_ind vz vs (S vn)} & \implies \text{vs n (nat\_ind vz vs vn)}
\end{align*}
\]
(c) It remains to give a typing rule for \texttt{nat\_ind}. We know that the third argument to \texttt{nat\_ind} is supposed to be a \texttt{Nat}, so that part is easy. The result type of a \texttt{nat\_ind} expression can be any type \(T\), since we could conceivably construct any value by induction on a natural number. We have filled in those parts of the typing rule below.

Your job is to complete the typing rule. Consider that this rule should be sound (i.e. satisfy preservation and progress) with respect to the operational semantics outlined above. For example, the term \texttt{Nat\_plus} defined in part (b) should be well-typed according to your rule.

\[
\begin{align*}
\Gamma \vdash tz : T & \quad \Gamma \vdash ts : \texttt{Nat} \rightarrow T \rightarrow T & \quad \Gamma \vdash tn : \texttt{Nat} \\
\Gamma \vdash \texttt{nat\_ind} tz ts tn : T
\end{align*}
\]
(d) Part (b) used \texttt{nat\_ind} to define the \texttt{Nat\_plus} function. Use \texttt{Nat\_plus} and \texttt{nat\_ind} to define multiplication of two numbers. We have provided the type of \texttt{Nat\_mult} to get you started:

\[
(* \text{Nat\_mult} : \text{Nat} \to \text{Nat} \to \text{Nat} *) \\\n\forall n:\text{Nat}. \forall m:\text{Nat}. \text{nat\_ind} 0 (\forall x:\text{Nat}. \forall p:\text{Nat}. \text{Nat\_plus} m p) n
\]

(e) A harder function to define using \texttt{nat\_ind} is natural number equality, a function \texttt{Nat\_eq} of type \texttt{Nat \to Nat \to Nat} such that \texttt{Nat\_eq n m} \Rightarrow 0 if \(n\) and \(m\) are different natural numbers and \texttt{nat\_eq n m} \Rightarrow 1 if they are the same.

We have started the definition. Fill in the two blanks to complete it.

\[
(* \text{Nat\_eq} : \text{Nat} \to (\text{Nat} \to \text{Nat}) *) \\\n\forall n:\text{Nat}. \\text{nat\_ind} (\forall m:\text{Nat}. \text{nat\_ind} 1 (\forall x:\text{Nat}. \forall y:\text{Nat}. 0) m) \\quad \text{nat\_ind} 0 (\forall p:\text{Nat}. \forall y:\text{Nat}. \text{eq} p) n
\]
8. (10 points) Subtyping

The rules for STLC with pairs and subtyping are given on page 24 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 $\text{Top} \ast \text{Top}$, $\text{A} \ast \text{Top}$, $\text{Top} \ast (\text{Top} \ast \text{Top})$, and $\text{Top} \ast (\text{A} \ast \text{A})$ would look like this (it happens to form a tree, but that is not necessary in general):

```
                Top*Top
               /     \
        A*Top   Top*(Top*Top)
             /     \
       Top*(A*A)
```

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

- $\text{Top} \rightarrow (A \ast B)$
- $\text{Top} \rightarrow (A \ast A)$
- $(B \ast A) \rightarrow (B \ast A)$
- $(A \ast B) \rightarrow (B \ast A)$
- $(B \ast A) \rightarrow \text{Top}$
- $\text{Top}$

*Answer:*

```
                Top
               /     \
        (B*A) \rightarrow Top   (A*B) \rightarrow (B*A)
               /     \
       Top \rightarrow (A*B)   (B*A) \rightarrow (B*A)
             /     \
       Top \rightarrow (A*A)
```
9. [Standard] (8 points) True or False
   For each question, indicate whether it is true or false. Very briefly justify your answer.

   (a) In the STLC with subtyping (see the rules on page 24) there exists a type \( T \) such that
       \( \lambda x: T. \ x \ x \) is typeable.
       True: \( T = \text{Top} \to \text{Top} \)

   (b) In the STLC with subtyping, there is at most one typing derivation for each term \( t \).
       False: Subsumption

   (c) In the STLC with subtyping and records, the empty record type \( \{ \} \) is a subtype of all other
       records.
       False: It is the supertype.

   (d) In the STLC with subtyping and records, it is sound (i.e. both preservation and progress still
       hold) to add the subtyping rule \( \text{Top} <: \{ \} \).
       True: The empty record, like \( \text{Top} \) supports no operations.
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).
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').

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').

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).

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

Hoare logic rules

\[
\begin{align*}
\langle \text{assn} \_{\text{sub}} \ X \ a \ Q \ X := a \ Q \rangle \quad &\text{(hoare\_asgn)} \\
\langle P \rangle \ \text{SKIP} \ \langle P \rangle \quad &\text{(hoare\_skip)} \\
\langle P \rangle \ c_1 \ C \ Q \quad &\text{(hoare\_seq)} \\
\langle P \rangle \ c_1; \ c_2 \ C \ R \quad &\text{(hoare\_seq)} \\
\langle P \rangle \ \text{IFB} \ b \ \text{THEN} \ c_1 \ \text{ELSE} \ c_2 \ FI \ C \ Q \quad &\text{(hoare\_if)} \\
\langle P \rangle \ \text{WHILE} \ b \ \text{DO} \ c \ \text{END} \ C \ P' \quad &\text{(hoare\_while)} \\
\langle P' \rangle \ c \ C \ Q' \quad &\text{(hoare\_consequence)} \\
\langle P' \rangle \ c \ C \ Q' \quad &\text{(hoare\_consequence\_pre)} \\
\langle P \rangle \ c \ C \ Q' \quad &\text{(hoare\_consequence\_post)} \\
\end{align*}
\]
Decorated programs

(a) \textbf{SKIP} is locally consistent if its precondition and postcondition are the same:

\[
\{\{ P \}\}
\text{SKIP}
\{\{ P \}\}
\]

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

\[
\{\{ P \}\}
\texttt{c1;}
\{\{ Q \}\}
\texttt{c2}
\{\{ R \}\}
\]

(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 \texttt{P} and \texttt{Q}) if the assertions at the top of its "then" and "else" branches are exactly \texttt{P /\ b} and \texttt{P /\ \neg b} and if its "then" branch is locally consistent (with respect to \texttt{P /\ b} and \texttt{Q}) and its "else" branch is locally consistent (with respect to \texttt{P /\ \neg b} and \texttt{Q}):

\[
\{\{ P \}\}
\text{IFB \texttt{b} THEN}
\{\{ P /\ b \}\}
\texttt{c1}
\{\{ Q \}\}
\text{ELSE}
\{\{ P /\ \neg b \}\}
\texttt{c2}
\{\{ Q \}\}
\text{FI}
\{\{ Q \}\}
\]
(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 $P$:

\[
\begin{align*}
\{\{ P \}\} \\
\text{WHILE } b \text{ DO} \\
\{\{ P \land b \}\} \\
c1 \\
\{\{ P \}\} \\
\text{END} \\
\{\{ P \land \neg b \}\}
\end{align*}
\]

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

\[
\begin{align*}
\{\{ P \}\} \neg\neg \\
\{\{ P' \}\}
\end{align*}
\]
STLC with Natural Numbers

Syntax

(* Types *) (* Terms *) (* Values *)
T ::= Nat ⊢ Nat t ::= x v ::= 0
| T → T | t t | \x:T. t
| \x:T. t | 0 | S t

Small-step operational semantics

value v2
-------------------------------------- (ST_AppAbs)
(\x:T.t12) v2 ==> [x:=v2]t12

  t1 ==> t1'
--------------------------------- (ST_App1)
t1 t2 ==> t1' t2

value v1
  t2 ==> t2'
--------------------------------- (ST_App2)
v1 t2 ==> v1 t2'

  t1 ==> t1'
--------------------------------- (ST_Succ)
S t1 ==> S t1'
Typing

\[ \Gamma \vdash x = T \]
\[ \Gamma \vdash x \in T \]
\[ \text{(T_Var)} \]

\[ \Gamma, x:T_{11} \vdash t_{12} \in T_{12} \]
\[ \Gamma \vdash \lambda x:T_{11}.t_{12} \in T_{11} \rightarrow T_{12} \]
\[ \text{(T_Abs)} \]

\[ \Gamma \vdash t_1 \in T_{11} \rightarrow T_{12} \]
\[ \Gamma \vdash t_2 \in T_{11} \]
\[ \Gamma \vdash t_1 \ t_2 \in T_{12} \]
\[ \text{(T_App)} \]

\[ \Gamma \vdash 0 \in \text{Nat} \]
\[ \text{(T_Zero)} \]

\[ \Gamma \vdash t \in \text{Nat} \]
\[ \Gamma \vdash S \ t \in \text{Nat} \]
\[ \text{(T_Succ)} \]
STLC with pairs and subtyping (excerpt)

Types

\[ T ::= \ldots \]
\[ | \text{Top} \]
\[ | T \rightarrow T \]
\[ | T * T \]

Subtyping relation

\[
\begin{align*}
S & <: U \quad U <: T \\
\text{----------------} & (S_{\text{Trans}}) \\
S & <: T \\
\text{------} & (S_{\text{Refl}}) \\
T & <: T \\
\text{--------} & (S_{\text{Top}}) \\
S & <: \text{Top} \\
\end{align*}
\]

\[
\begin{align*}
S1 & <: T1 \quad S2 <: T2 \\
\text{----------------} & (S_{\text{Prod}}) \\
S1*S2 & <: T1*T2 \\
\end{align*}
\]

\[
\begin{align*}
T1 & <: S1 \quad S2 <: T2 \\
\text{----------------} & (S_{\text{Arrow}}) \\
S1->S2 & <: T1->T2 \\
\end{align*}
\]