IMP

SIMPLE IMPERATIVE PROGRAMS

In this chapter, we take a more serious look at how to use Coq to study other things. Our case study is a *simple imperative programming language* called Imp, embodying a tiny core fragment of conventional mainstream languages such as C and Java. Here is a familiar mathematical function written in Imp.

```
Z := X;
Y := 1;
while ~(Z = 0) do
  Y := Y × Z;
  Z := Z - 1
end
```

We concentrate here on defining the *syntax* and *semantics* of Imp; later chapters in *Programming Language Foundations* (*Software Foundations*, volume 2) develop a theory of *program equivalence* and introduce *Hoare Logic*, a widely used logic for reasoning about imperative programs.

```
Set Warnings "-notation-overridden,-parsing".
From Coq Require Import Bool.Bool.
From Coq Require Import Init.Nat.
From Coq Require Import Arith.Arith.
From Coq Require Import Arith.EqNat.
From Coq Require Import Lia.
From Coq Require Import Lists.List.
From Coq Require Import Strings.String.
Import ListNotations.

From LF Require Import Maps.
```

Arithmetic and Boolean Expressions

We'll present Imp in three parts: first a core language of *arithmetic and boolean expressions*, then an extension of these expressions with *variables*, and finally a language of *commands* including assignment, conditions, sequencing, and loops.

Syntax

```
Module AExp.
```

These two definitions specify the *abstract syntax* of arithmetic and boolean expressions.

```
Inductive aexp : Type :=
  | ANum (n : nat)
  | APlus (a1 a2 : aexp)
  | AMinus (a1 a2 : aexp)
  | AMult (a1 a2 : aexp).

Inductive bexp : Type :=
  | BTrue
  | BFalse
  | BEq (a1 a2 : aexp)
  | BLe (a1 a2 : aexp)
  | BNot (b : bexp)
  | BAnd (b1 b2 : bexp).
```

In this chapter, we'll mostly elide the translation from the concrete syntax that a programmer would actually write to these abstract syntax trees -- the process that, for example, would translate the string `"1 + 2 × 3"` to the AST

```
APlus (ANum 1) (AMult (ANum 2) (ANum 3)).
```

The optional chapter ImpParser develops a simple lexical analyzer and parser that can perform this translation. You do *not* need to understand that chapter to understand this one, but if you haven't already taken a course where these techniques are covered (e.g., a compilers course) you may want to skim it.

For comparison, here's a conventional BNF (Backus-Naur Form) grammar defining the same abstract syntax:

```
a := nat
     | a + a
     | a - a
     | a × a

b := true
     | false
     | a = a
     | a ≤ a
     | ¬b
     | b && b
```

Compared to the Coq version above...

- The BNF is more informal -- for example, it gives some suggestions about the surface syntax of expressions (like the fact that the addition operation is written with an infix `+`) while leaving other aspects of lexical analysis and parsing (like the relative precedence of `+`, `-`, and `×`, the use of parens to group subexpressions, etc.) unspecified. Some additional information -- and human intelligence -- would be required to turn this description into a formal definition, e.g., for implementing a compiler.

  The Coq version consistently omits all this information and concentrates on the abstract syntax only.

- Conversely, the BNF version is lighter and easier to read. Its informality makes it flexible, a big advantage in situations like discussions at the blackboard, where conveying general ideas is more important than getting every detail nailed down precisely.

  Indeed, there are dozens of BNF-like notations and people switch freely among them, usually without bothering to say which kind of BNF they're using because there is no need to: a rough-and-ready informal understanding is all that's important.

It's good to be comfortable with both sorts of notations: informal ones for communicating between humans and formal ones for carrying out implementations and proofs.

Evaluation

Evaluating an arithmetic expression produces a number.

```
Fixpoint aeval (a : aexp) : nat :=
  match a with
  | ANum n ⇒ n
  | APlus a1 a2 ⇒ (aeval a1) + (aeval a2)
  | AMinus a1 a2 ⇒ (aeval a1) - (aeval a2)
  | AMult a1 a2 ⇒ (aeval a1) × (aeval a2)
  end.

Example test_aeval1:
  aeval (APlus (ANum 2) (ANum 2)) = 4.
```

Similarly, evaluating a boolean expression yields a boolean.

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

Optimization

We haven't defined very much yet, but we can already get some mileage out of the definitions. Suppose we define a function that takes an arithmetic expression and slightly simplifies it, changing every occurrence of `0 + e` (i.e., `(APlus (ANum 0) e)` into just `e`.

```
Fixpoint optimize_0plus (a:aexp) : aexp :=
  match a with
  | ANum n ⇒ ANum n
  | APlus (ANum 0) e2 ⇒ optimize_0plus e2
  | APlus e1 e2 ⇒ APlus (optimize_0plus e1) (optimize_0plus e2)
  | AMinus e1 e2 ⇒ AMinus (optimize_0plus e1) (optimize_0plus e2)
  | AMult e1 e2 ⇒ AMult (optimize_0plus e1) (optimize_0plus e2)
  end.
```

To make sure our optimization is doing the right thing we can test it on some examples and see if the output looks OK.

```
Example test_optimize_0plus:
  optimize_0plus (APlus (ANum 2)
                        (APlus (ANum 0)
                               (APlus (ANum 0) (ANum 1))))
  = APlus (ANum 2) (ANum 1).
```

But if we want to be sure the optimization is correct -- i.e., that evaluating an optimized expression gives the same result as the original -- we should prove it.

```
Theorem optimize_0plus_sound: ∀ a,
  aeval (optimize_0plus a) = aeval a.
```

Coq Automation

The amount of repetition in this last proof is a little annoying. And if either the language of arithmetic expressions or the optimization being proved sound were significantly more complex, it would start to be a real problem.

So far, we've been doing all our proofs using just a small handful of Coq's tactics and completely ignoring its powerful facilities for constructing parts of proofs automatically. This section introduces some of these facilities, and we will see more over the next several chapters. Getting used to them will take some energy -- Coq's automation is a power tool -- but it will allow us to scale up our efforts to more complex definitions and more interesting properties without becoming overwhelmed by boring, repetitive, low-level details.

Tacticals

Tacticals is Coq's term for tactics that take other tactics as arguments -- "higher-order tactics," if you will.

The `try` Tactical

If `T` is a tactic, then `try T` is a tactic that is just like `T` except that, if `T` fails, `try T` *successfully* does nothing at all (rather than failing).

```
Theorem silly1 : ∀ ae, aeval ae = aeval ae.
Proof. try reflexivity. (* This just does reflexivity. *) Qed.

Theorem silly2 : ∀ (P : Prop), P → P.
Proof.
  intros P HP.
  try reflexivity. (* Just reflexivity would have failed. *)
  apply HP. (* We can still finish the proof in some other way. *)
Qed.
```

There is no real reason to use `try` in completely manual proofs like these, but it is very useful for doing automated proofs in conjunction with the `;` tactical, which we show next.

The `;` Tactical (Simple Form)

In its most common form, the `;` tactical takes two tactics as arguments. The compound tactic `T;T'` first performs `T` and then performs `T'` on *each subgoal* generated by `T`.

For example, consider the following trivial lemma:

```
Lemma foo : ∀ n, 0 <=? n = true.
Proof.
  intros.
  destruct n.
    (* Leaves two subgoals, which are discharged identically...  *)
    - (* n=0 *) simpl. reflexivity.
    - (* n=Sn' *) simpl. reflexivity.
Qed.
```

We can simplify this proof using the `;` tactical:

```
Lemma foo' : ∀ n, 0 <=? n = true.
Proof.
  intros.
  (* destruct the current goal *)
  destruct n;
  (* then simpl each resulting subgoal *)
  simpl;
  (* and do reflexivity on each resulting subgoal *)
  reflexivity.
Qed.
```

Using `try` and `;` together, we can get rid of the repetition in the proof that was bothering us a little while ago.

```
Theorem optimize_0plus_sound': ∀ a,
  aeval (optimize_0plus a) = aeval a.
Proof.
  intros a.
  induction a;
    (* Most cases follow directly by the IH... *)
    try (simpl; rewrite IHa1; rewrite IHa2; reflexivity).
    (* ... but the remaining cases -- ANum and APlus --
       are different: *)
  - (* ANum *) reflexivity.
  - (* APlus *)
    destruct a1 eqn:Ea1;
      (* Again, most cases follow directly by the IH: *)
      try (simpl; simpl in IHa1; rewrite IHa1;
           rewrite IHa2; reflexivity).
    (* The interesting case, on which the try...
       does nothing, is when e1 = ANum n. In this
       case, we have to destruct n (to see whether
       the optimization applies) and rewrite with the
       induction hypothesis. *)
    + (* a1 = ANum n *) destruct n eqn:En;
      simpl; rewrite IHa2; reflexivity. Qed.
```

Coq experts often use this "`...; try...`" idiom after a tactic like `induction` to take care of many similar cases all at once. Naturally, this practice has an analog in informal proofs. For example, here is an informal proof of the optimization theorem that matches the structure of the formal one:

Theorem: For all arithmetic expressions `a`,

```
    aeval (optimize_0plus a) = aeval a.
```

Proof: By induction on `a`. Most cases follow directly from the IH. The remaining cases are as follows:

- Suppose `a = ANum n` for some `n`. We must show

  ```
  aeval (optimize_0plus (ANum n)) = aeval (ANum n).
  ```

  This is immediate from the definition of `optimize_0plus`.

- Suppose `a = APlus a1 a2` for some a_1 and a_2. We must show

  ```
  aeval (optimize_0plus (APlus a1 a2)) = aeval (APlus a1 a2).
  ```

  Consider the possible forms of a_1. For most of them, `optimize_0plus` simply calls itself recursively for the subexpressions and rebuilds a new expression of the same form as a_1; in these cases, the result follows directly from the IH.

  The interesting case is when a_1 `= ANum n` for some `n`. If `n = 0`, then

  ```
  optimize_0plus (APlus a1 a2) = optimize_0plus a2
  ```

  and the IH for a_2 is exactly what we need. On the other hand, if `n = S n'` for some `n'`, then again `optimize_0plus` simply calls itself recursively, and the result follows from the IH. □

However, this proof can still be improved: the first case (for `a = ANum n`) is very trivial -- even more trivial than the cases that we said simply followed from the IH -- yet we have chosen to write it out in full. It would be better and clearer to drop it and just say, at the top, "Most cases are either immediate or direct from the IH. The only interesting case is the one for `APlus`..." We can make the same improvement in our formal proof too. Here's how it looks:

```
Theorem optimize_0plus_sound'': ∀ a,
  aeval (optimize_0plus a) = aeval a.
Proof.
  intros a.
  induction a;
    (* Most cases follow directly by the IH *)
    try (simpl; rewrite IHa1; rewrite IHa2; reflexivity);
    (* ... or are immediate by definition *)
    try reflexivity.
  (* The interesting case is when a = APlus a1 a2. *)
  - (* APlus *)
    destruct a1; try (simpl; simpl in IHa1; rewrite IHa1;
                      rewrite IHa2; reflexivity).
    + (* a1 = ANum n *) destruct n;
      simpl; rewrite IHa2; reflexivity. Qed.
```

The `;` Tactical (General Form)

The `;` tactical also has a more general form than the simple `T;T'` we've seen above. If `T`, T_1, ..., `Tn` are tactics, then

```
T; [T1 | T2 | ... | Tn]
```

is a tactic that first performs `T` and then performs T_1 on the first subgoal generated by `T`, performs T_2 on the second subgoal, etc.

So `T;T'` is just special notation for the case when all of the `Ti`'s are the same tactic; i.e., `T;T'` is shorthand for:

```
T; [T' | T' | ... | T']
```

The `repeat` Tactical

The `repeat` tactical takes another tactic and keeps applying this tactic until it fails to make progress. Here is an example showing that `10` is in a long list using `repeat`.

```
Theorem In10 : In 10 [1;2;3;4;5;6;7;8;9;10].
Proof.
  repeat (try (left; reflexivity); right).
Qed.
```

The tactic `repeat T` never fails: if the tactic `T` doesn't apply to the original goal, then repeat still succeeds without changing the original goal (i.e., it repeats zero times).

```
Theorem In10' : In 10 [1;2;3;4;5;6;7;8;9;10].
Proof.
  repeat simpl.
  repeat (left; reflexivity).
  repeat (right; try (left; reflexivity)).
Qed.
```

The tactic `repeat T` also does not have any upper bound on the number of times it applies `T`. If `T` is a tactic that always succeeds (and makes progress), then repeat `T` will loop forever.

```
Theorem repeat_loop : ∀ (m n : nat),
    m + n = n + m.
Proof.
  intros m n.
  (* Uncomment the next line to see the infinite loop occur.
     In Proof General, C-c C-c will break out of the loop. *)
  (* repeat rewrite Nat.add_comm. *)
Admitted.
```

While evaluation in Coq's term language, Gallina, is guaranteed to terminate, tactic evaluation is not! This does not affect Coq's logical consistency, however, since the job of `repeat` and other tactics is to guide Coq in constructing proofs; if the construction process diverges (i.e., it does not terminate), this simply means that we have failed to construct a proof, not that we have constructed a wrong one.

Exercise: 3 stars, standard (optimize_0plus_b_sound)

Since the `optimize_0plus` transformation doesn't change the value of `aexp`s, we should be able to apply it to all the `aexp`s that appear in a `bexp` without changing the `bexp`'s value. Write a function that performs this transformation on `bexp`s and prove it is sound. Use the tacticals we've just seen to make the proof as elegant as possible.

```
Fixpoint optimize_0plus_b (b : bexp) : bexp
  (* REPLACE THIS LINE WITH ":= _your_definition_ ." *). Admitted.

Theorem optimize_0plus_b_sound : ∀ b,
  beval (optimize_0plus_b b) = beval b.
Proof.
  (* FILL IN HERE *) Admitted.
□
```

Exercise: 4 stars, standard, optional (optimize)

Design exercise: The optimization implemented by our `optimize_0plus` function is only one of many possible optimizations on arithmetic and boolean expressions. Write a more sophisticated optimizer and prove it correct. (You will probably find it easiest to start small -- add just a single, simple optimization and its correctness proof -- and build up to something more interesting incrementially.)

```
(* FILL IN HERE *)
□
```

Defining New Tactic Notations

Coq also provides several ways of "programming" tactic scripts.

- The `Tactic Notation` idiom illustrated below gives a handy way to define "shorthand tactics" that bundle several tactics into a single command.
- For more sophisticated programming, Coq offers a built-in language called `Ltac` with primitives that can examine and modify the proof state. The details are a bit too complicated to get into here (and it is generally agreed that `Ltac` is not the most beautiful part of Coq's design!), but they can be found in the reference manual and other books on Coq, and there are many examples of `Ltac` definitions in the Coq standard library that you can use as examples.
- There is also an OCaml API, which can be used to build tactics that access Coq's internal structures at a lower level, but this is seldom worth the trouble for ordinary Coq users.

The `Tactic Notation` mechanism is the easiest to come to grips with, and it offers plenty of power for many purposes. Here's an example.

```
Tactic Notation "simpl_and_try" tactic(c) :=
  simpl;
  try c.
```

This defines a new tactical called `simpl_and_try` that takes one tactic `c` as an argument and is defined to be equivalent to the tactic `simpl; try c`. Now writing "`simpl_and_try reflexivity.`" in a proof will be the same as writing "`simpl; try reflexivity.`"

The `omega` Tactic

The `omega` tactic implements a decision procedure for a subset of first-order logic called *Presburger arithmetic*. It is based on the Omega algorithm invented by William Pugh [Pugh 1991].

If the goal is a universally quantified formula made out of

- numeric constants, addition (`+` and `S`), subtraction (`-` and `pred`), and multiplication by constants (this is what makes it Presburger arithmetic),
- equality (`=` and `≠`) and ordering (`≤`), and
- the logical connectives `∧`, `∨`, `¬`, and `→`,

then invoking `omega` will either solve the goal or fail, meaning that the goal is actually false. (If the goal is *not* of this form, `omega` will also fail.)

```
Example silly_presburger_example : ∀ m n o p,
  m + n ≤ n + o ∧ o + 3 = p + 3 →
  m ≤ p.
Proof.
  intros. lia.
Qed.

Example plus_comm__omega : ∀ m n,
    m + n = n + m.
Proof.
  intros. lia.
Qed.

Example plus_assoc__omega : ∀ m n p,
    m + (n + p) = m + n + p.
Proof.
  intros. lia.
Qed.
```

(Note the `From Coq Require Import Lia.` at the top of the file.)

A Few More Handy Tactics

Finally, here are some miscellaneous tactics that you may find convenient.

- `clear H`: Delete hypothesis `H` from the context.
- `subst x`: For a variable `x`, find an assumption `x = e` or `e = x` in the context, replace `x` with `e` throughout the context and current goal, and clear the assumption.
- `subst`: Substitute away *all* assumptions of the form `x = e` or `e = x` (where `x` is a variable).
- `rename... into...`: Change the name of a hypothesis in the proof context. For example, if the context includes a variable named `x`, then `rename x into y` will change all occurrences of `x` to `y`.
- `assumption`: Try to find a hypothesis `H` in the context that exactly matches the goal; if one is found, solve the goal.
- `contradiction`: Try to find a hypothesis `H` in the current context that is logically equivalent to `False`. If one is found, solve the goal.
- `constructor`: Try to find a constructor `c` (from some `Inductive` definition in the current environment) that can be applied to solve the current goal. If one is found, behave like `apply c`.

We'll see examples of all of these as we go along.

Evaluation as a Relation

We have presented `aeval` and `beval` as functions defined by `Fixpoints`. Another way to think about evaluation -- one that we will see is often more flexible -- is as a *relation* between expressions and their values. This leads naturally to `Inductive` definitions like the following one for arithmetic expressions...

```
Module aevalR_first_try.

Inductive aevalR : aexp → nat → Prop :=
  | E_ANum n :
      aevalR (ANum n) n
  | E_APlus (e1 e2: aexp) (n1 n2: nat) :
      aevalR e1 n1 →
      aevalR e2 n2 →
      aevalR (APlus e1 e2) (n1 + n2)
  | E_AMinus (e1 e2: aexp) (n1 n2: nat) :
      aevalR e1 n1 →
      aevalR e2 n2 →
      aevalR (AMinus e1 e2) (n1 - n2)
  | E_AMult (e1 e2: aexp) (n1 n2: nat) :
      aevalR e1 n1 →
      aevalR e2 n2 →
      aevalR (AMult e1 e2) (n1 × n2).

Module HypothesisNames.

(* A small notational aside. We could also write the definition of
   aevalR as follow, with explicit names for the hypotheses in each
   case: *)

Inductive aevalR : aexp → nat → Prop :=
  | E_ANum n :
      aevalR (ANum n) n
  | E_APlus (e1 e2: aexp) (n1 n2: nat)
      (H1 : aevalR e1 n1)
      (H2 : aevalR e2 n2) :
      aevalR (APlus e1 e2) (n1 + n2)
  | E_AMinus (e1 e2: aexp) (n1 n2: nat)
      (H1 : aevalR e1 n1)
      (H2 : aevalR e2 n2) :
      aevalR (AMinus e1 e2) (n1 - n2)
  | E_AMult (e1 e2: aexp) (n1 n2: nat)
      (H1 : aevalR e1 n1)
      (H2 : aevalR e2 n2) :
      aevalR (AMult e1 e2) (n1 × n2).
```

This style gives us more control over the names that Coq chooses during proofs involving `aevalR`, at the cost of making the definition a little more verbose.

```
End HypothesisNames.
```

It will be convenient to have an infix notation for `aevalR`. We'll write `e ==> n` to mean that arithmetic expression `e` evaluates to value `n`.

```
Notation "e '==>' n"
         := (aevalR e n)
            (at level 90, left associativity)
         : type_scope.

End aevalR_first_try.
```

As we saw in IndProp in our case study of regular expressions, Coq provides a way to use this notation in the definition of `aevalR` itself.

```
Reserved Notation "e '==>' n" (at level 90, left associativity).

Inductive aevalR : aexp → nat → Prop :=
  | E_ANum (n : nat) :
      (ANum n) ==> n
  | E_APlus (e1 e2 : aexp) (n1 n2 : nat) :
      (e1 ==> n1) → (e2 ==> n2) → (APlus e1 e2) ==> (n1 + n2)
  | E_AMinus (e1 e2 : aexp) (n1 n2 : nat) :
      (e1 ==> n1) → (e2 ==> n2) → (AMinus e1 e2) ==> (n1 - n2)
  | E_AMult (e1 e2 : aexp) (n1 n2 : nat) :
      (e1 ==> n1) → (e2 ==> n2) → (AMult e1 e2) ==> (n1 × n2)

  where "e '==>' n" := (aevalR e n) : type_scope.
```

Inference Rule Notation

In informal discussions, it is convenient to write the rules for `aevalR` and similar relations in the more readable graphical form of *inference rules*, where the premises above the line justify the conclusion below the line (we have already seen them in the IndProp chapter).

For example, the constructor `E_APlus`...

```
  | E_APlus : ∀ (e1 e2: aexp) (n1 n2: nat),
      aevalR e1 n1 →
      aevalR e2 n2 →
      aevalR (APlus e1 e2) (n1 + n2)
```

...would be written like this as an inference rule:

$$\frac{e_1 \texttt{ ==> } n_1 \qquad e_2 \texttt{ ==> } n_2}{\texttt{APlus } e_1\ e_2 \texttt{ ==> } n_1+n_2}\ \text{(E\_APlus)}$$

Formally, there is nothing deep about inference rules: they are just implications. You can read the rule name on the right as the name of the constructor and read each of the linebreaks between the premises above the line (as well as the line itself) as →. All the variables mentioned in the rule (e_1, n_1, etc.) are implicitly bound by universal quantifiers at the beginning. (Such variables are often called *metavariables* to distinguish them from the variables of the language we are defining. At the moment, our arithmetic expressions don't include variables, but we'll soon be adding them.) The whole collection of rules is understood as being wrapped in an `Inductive` declaration. In informal prose, this is either elided or else indicated by saying something like "Let `aevalR` be the smallest relation closed under the following rules...".

For example, `==>` is the smallest relation closed under these rules:

$$\frac{}{\texttt{ANum } n \texttt{ ==> } n}\ \text{(E\_ANum)}$$

$$\frac{e_1 \texttt{ ==> } n_1 \qquad e_2 \texttt{ ==> } n_2}{\texttt{APlus } e_1\ e_2 \texttt{ ==> } n_1+n_2}\ \text{(E\_APlus)}$$

$$\frac{e_1 \texttt{ ==> } n_1 \qquad e_2 \texttt{ ==> } n_2}{\texttt{AMinus } e_1\ e_2 \texttt{ ==> } n_1-n_2}\ \text{(E\_AMinus)}$$

$$\frac{e_1 \texttt{ ==> } n_1 \qquad e_2 \texttt{ ==> } n_2}{\texttt{AMult } e_1\ e_2 \texttt{ ==> } n_1*n_2}\ \text{(E\_AMult)}$$

Exercise: 1 star, standard, optional (beval rules)

Here, again, is the Coq definition of the `beval` function:

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

Write out a corresponding definition of boolean evaluation as a relation (in inference rule notation).

```
(* FILL IN HERE *)

(* Do not modify the following line: *)
Definition manual_grade_for_beval_rules : option (nat×string) := None.
```

□

Equivalence of the Definitions

It is straightforward to prove that the relational and functional definitions of evaluation agree:

```
Theorem aeval_iff_aevalR : ∀ a n,
  (a ==> n) ↔ aeval a = n.
```

We can make the proof quite a bit shorter by making more use of tacticals.

```
Theorem aeval_iff_aevalR' : ∀ a n,
  (a ==> n) ↔ aeval a = n.
Proof.
  (* WORKED IN CLASS *)
  split.
  - (* -> *)
    intros H; induction H; subst; reflexivity.
  - (* <- *)
    generalize dependent n.
    induction a; simpl; intros; subst; constructor;
```

```
      try apply IHa1; try apply IHa2; reflexivity.
Qed.
```

Exercise: 3 stars, standard (bevalR)

Write a relation `bevalR` in the same style as `aevalR`, and prove that it is equivalent to `beval`.

```
Reserved Notation "e '==>b' b" (at level 90, left associativity).
Inductive bevalR: bexp → bool → Prop :=
(* FILL IN HERE *)
where "e '==>b' b" := (bevalR e b) : type_scope
.

Lemma beval_iff_bevalR : ∀ b bv,
  b ==>b bv ↔ beval b = bv.
Proof.
  (* FILL IN HERE *) Admitted.
□

End AExp.
```

Computational vs. Relational Definitions

For the definitions of evaluation for arithmetic and boolean expressions, the choice of whether to use functional or relational definitions is mainly a matter of taste: either way works.

However, there are circumstances where relational definitions of evaluation work much better than functional ones.

```
Module aevalR_division.
```

For example, suppose that we wanted to extend the arithmetic operations with division:

```
Inductive aexp : Type :=
  | ANum (n : nat)
  | APlus (a1 a2 : aexp)
  | AMinus (a1 a2 : aexp)
  | AMult (a1 a2 : aexp)
  | ADiv (a1 a2 : aexp). (* <--- NEW *)
```

Extending the definition of `aeval` to handle this new operation would not be straightforward (what should we return as the result of `ADiv (ANum 5) (ANum 0)`?). But extending `aevalR` is very easy.

```
Reserved Notation "e '==>' n"
                  (at level 90, left associativity).

Inductive aevalR : aexp → nat → Prop :=
  | E_ANum (n : nat) :
      (ANum n) ==> n
  | E_APlus (a1 a2 : aexp) (n1 n2 : nat) :
      (a1 ==> n1) → (a2 ==> n2) → (APlus a1 a2) ==> (n1 + n2)
  | E_AMinus (a1 a2 : aexp) (n1 n2 : nat) :
      (a1 ==> n1) → (a2 ==> n2) → (AMinus a1 a2) ==> (n1 - n2)
  | E_AMult (a1 a2 : aexp) (n1 n2 : nat) :
      (a1 ==> n1) → (a2 ==> n2) → (AMult a1 a2) ==> (n1 × n2)
  | E_ADiv (a1 a2 : aexp) (n1 n2 n3 : nat) : (* <----- NEW *)
      (a1 ==> n1) → (a2 ==> n2) → (n2 > 0) →
      (mult n2 n3 = n1) → (ADiv a1 a2) ==> n3

where "a '==>' n" := (aevalR a n) : type_scope.
```

Notice that the evaluation relation has now become *partial*: There are some inputs for which it simply does not specify an output.

```
End aevalR_division.

Module aevalR_extended.
```

Or suppose that we want to extend the arithmetic operations by a nondeterministic number generator `any` that, when evaluated, may yield any number. Note that this is not the same as making a *probabilistic* choice among all possible numbers -- we're not specifying any particular probability distribution for the results, just saying what results are *possible*.

```
Reserved Notation "e '==>' n" (at level 90, left associativity).

Inductive aexp : Type :=
  | AAny (* <--- NEW *)
  | ANum (n : nat)
  | APlus (a1 a2 : aexp)
  | AMinus (a1 a2 : aexp)
  | AMult (a1 a2 : aexp).
```

Again, extending `aeval` would be tricky, since now evaluation is *not* a deterministic function from expressions to numbers, but extending `aevalR` is no problem...

```
Inductive aevalR : aexp → nat → Prop :=
  | E_Any (n : nat) :
      AAny ==> n (* <--- NEW *)
  | E_ANum (n : nat) :
      (ANum n) ==> n
  | E_APlus (a1 a2 : aexp) (n1 n2 : nat) :
      (a1 ==> n1) → (a2 ==> n2) → (APlus a1 a2) ==> (n1 + n2)
  | E_AMinus (a1 a2 : aexp) (n1 n2 : nat) :
      (a1 ==> n1) → (a2 ==> n2) → (AMinus a1 a2) ==> (n1 - n2)
  | E_AMult (a1 a2 : aexp) (n1 n2 : nat) :
      (a1 ==> n1) → (a2 ==> n2) → (AMult a1 a2) ==> (n1 × n2)

where "a '==>' n" := (aevalR a n) : type_scope.

End aevalR_extended.
```

At this point you maybe wondering: which style should I use by default? In the examples we've just seen, relational definitions turned out to be more useful than functional ones. For situations like these, where the thing being defined is not easy to express as a function, or indeed where it is *not* a function, there is no real choice. But what about when both styles are workable?

One point in favor of relational definitions is that they can be more elegant and easier to understand.

Another is that Coq automatically generates nice inversion and induction principles from `Inductive` definitions.

On the other hand, functional definitions can often be more convenient:

- Functions are by definition deterministic and defined on all arguments; for a relation we have to *prove* these properties explicitly if we need them.
- With functions we can also take advantage of Coq's computation mechanism to simplify expressions during proofs.

Furthermore, functions can be directly "extracted" from Gallina to executable code in OCaml or Haskell.

Ultimately, the choice often comes down to either the specifics of a particular situation or simply a question of taste. Indeed, in large Coq developments it is common to see a definition given in *both* functional and relational styles, plus a lemma stating that the two coincide, allowing further proofs to switch from one point of view to the other at will.

Expressions With Variables

Now we return to defining Imp. The next thing we need to do is to enrich our arithmetic and boolean expressions with variables. To keep things simple, we'll assume that all variables are global and that they only hold numbers.

States

Since we'll want to look variables up to find out their current values, we'll reuse maps from the Maps chapter, and `string`s will be used to represent variables in Imp.

A *machine state* (or just *state*) represents the current values of *all* variables at some point in the execution of a program.

For simplicity, we assume that the state is defined for *all* variables, even though any given program is only going to mention a finite number of them. The state captures all of the information stored in memory. For Imp programs, because each variable stores a natural number, we can represent the state as a mapping from strings to `nat`, and will use `0` as default value in the store. For more complex programming languages, the state might have more structure.

```
Definition state := total_map nat.
```

Syntax

We can add variables to the arithmetic expressions we had before by simply adding one more constructor:

```
Inductive aexp : Type :=
  | ANum (n : nat)
  | AId (x : string) (* <--- NEW *)
  | APlus (a1 a2 : aexp)
  | AMinus (a1 a2 : aexp)
  | AMult (a1 a2 : aexp).
```

Defining a few variable names as notational shorthands will make examples easier to read:

```
Definition W : string := "W".
Definition X : string := "X".
Definition Y : string := "Y".
Definition Z : string := "Z".
```

(This convention for naming program variables (`X`, `Y`, `Z`) clashes a bit with our earlier use of uppercase letters for types. Since we're not using polymorphism heavily in the chapters developed to Imp, this overloading should not cause confusion.)

The definition of `bexp`s is unchanged (except that it now refers to the new `aexp`s):

```
Inductive bexp : Type :=
  | BTrue
  | BFalse
  | BEq (a1 a2 : aexp)
  | BLe (a1 a2 : aexp)
  | BNot (b : bexp)
  | BAnd (b1 b2 : bexp).
```

Notations

To make Imp programs easier to read and write, we introduce some notations and implicit coercions. You do not need to understand exactly what these declarations do. Briefly, though:

- The `Coercion` declaration stipulates that a function (or constructor) can be implicitly used by the type system to coerce a value of the input type to a value of the output type. For instance, the coercion declaration for `AId` allows us to use plain strings when an `aexp` is expected; the string will implicitly be wrapped with `AId`.
- `Declare Custom Entry com` tells Coq to create a new "custom grammar" for parsing Imp expressions and programs. The first notation declaration after this tells Coq that anything between `<{` and `}>` should be parsed using the Imp grammar. Again, it is not necessary to understand the details, but it is important to recognize that we are defining *new* interpretations for some familiar operators like `+`, `-`, `×`, `=`, `≤`, etc., when they occur between `<{` and `}>`.

```
Coercion AId : string >-> aexp.
Coercion ANum : nat >-> aexp.

Declare Custom Entry com.
Declare Scope com_scope.
Notation "<{ e }>" := e (at level 0, e custom com at level 99) : com_scope.
Notation "( x )" := x (in custom com, x at level 99) : com_scope.
Notation "x" := x (in custom com at level 0, x constr at level 0) : com_scope.
Notation "f x .. y" := (.. (f x) .. y)
                  (in custom com at level 0, only parsing,
                  f constr at level 0, x constr at level 9,
                  y constr at level 9) : com_scope.
Notation "x + y" := (APlus x y) (in custom com at level 50, left associativity).
Notation "x - y" := (AMinus x y) (in custom com at level 50, left associativity).
Notation "x * y" := (AMult x y) (in custom com at level 40, left associativity).
Notation "'true'" := true (at level 1).
Notation "'true'" := BTrue (in custom com at level 0).
Notation "'false'" := false (at level 1).
Notation "'false'" := BFalse (in custom com at level 0).
Notation "x <= y" := (BLe x y) (in custom com at level 70, no associativity).
Notation "x = y" := (BEq x y) (in custom com at level 70, no associativity).
Notation "x && y" := (BAnd x y) (in custom com at level 80, left associativity).
Notation "'~' b" := (BNot b) (in custom com at level 75, right associativity).

Open Scope com_scope.
```

We can now write `3 + (X × 2)` instead of `APlus 3 (AMult X 2)`, and `true && ~(X ≤ 4)` instead of `BAnd true (BNot (BLe X 4))`.

```
Definition example_aexp : aexp := <{ 3 + (X × 2) }>.
Definition example_bexp : bexp := <{ true && ¬(X ≤ 4) }>.
```

One downside of these and notation tricks -- coercions in particular -- is that they can make it a little harder for humans to calculate the types of expressions. If you ever find yourself confused, try doing `Set Printing Coercions` to see exactly what is going on.

```
Print example_bexp.
(* ===> example_bexp = <{(true && ~ (X <= 4))}> *)

Set Printing Coercions.
Print example_bexp.
(* ===> example_bexp = <{(true && ~ (AId X <= ANum 4))}> *)

Unset Printing Coercions.
```

Evaluation

The arith and boolean evaluators are extended to handle variables in the obvious way, taking a state as an extra argument:

```
Fixpoint aeval (st : state) (a : aexp) : nat :=
  match a with
  | ANum n ⇒ n
  | AId x ⇒ st x (* <--- NEW *)
  | <{a₁ + a₂}> ⇒ (aeval st a₁) + (aeval st a₂)
  | <{a₁ - a₂}> ⇒ (aeval st a₁) - (aeval st a₂)
  | <{a₁ × a₂}> ⇒ (aeval st a₁) × (aeval st a₂)
  end.

Fixpoint beval (st : state) (b : bexp) : bool :=
  match b with
  | <{true}> ⇒ true
  | <{false}> ⇒ false
  | <{a₁ = a₂}> ⇒ (aeval st a₁) =? (aeval st a₂)
  | <{a₁ ≤ a₂}> ⇒ (aeval st a₁) <=? (aeval st a₂)
  | <{¬ b₁}> ⇒ negb (beval st b₁)
  | <{b₁ && b₂}> ⇒ andb (beval st b₁) (beval st b₂)
  end.
```

We specialize our notation for total maps to the specific case of states, i.e. using `(_ !-> 0)` as empty state.

```
Definition empty_st := (_ !-> 0).
```

Now we can add a notation for a "singleton state" with just one variable bound to a value.

```
Notation "x '!->' v" := (t_update empty_st x v) (at level 100).

Example aexp1 :
    aeval (X !-> 5) <{ (3 + (X × 2))}>
  = 13.
+

Example bexp1 :
    beval (X !-> 5) <{ true && ¬(X ≤ 4)}>
  = true.
+
```

Commands

Now we are ready define the syntax and behavior of Imp *commands* (sometimes called *statements*).

Syntax

Informally, commands `c` are described by the following BNF grammar.

```
    c := skip | x := a | c ; c | if b then c else c end
       | while b do c end
```

Here is the formal definition of the abstract syntax of commands:

```
Inductive com : Type :=
  | CSkip
  | CAss (x : string) (a : aexp)
  | CSeq (c₁ c₂ : com)
  | CIf (b : bexp) (c₁ c₂ : com)
  | CWhile (b : bexp) (c : com).
```

As for expressions, we can use a few `Notation` declarations to make reading and writing Imp programs more convenient.

```
Notation "'skip'" :=
         CSkip (in custom com at level 0) : com_scope.
Notation "x := y" :=
         (CAss x y)
            (in custom com at level 0, x constr at level 0,
             y at level 85, no associativity) : com_scope.
Notation "x ; y" :=
         (CSeq x y)
           (in custom com at level 90, right associativity) : com_scope.
Notation "'if' x 'then' y 'else' z 'end'" :=
         (CIf x y z)
           (in custom com at level 89, x at level 99,
            y at level 99, z at level 99) : com_scope.
Notation "'while' x 'do' y 'end'" :=
         (CWhile x y)
            (in custom com at level 89, x at level 99, y at level 99) : com_scope.
```

For example, here is the factorial function again, written as a formal definition to Coq:

```
Definition fact_in_coq : com :=
  <{ Z := X;
     Y := 1;
     while ¬(Z = 0) do
       Y := Y × Z;
       Z := Z - 1
     end }>.

Print fact_in_coq.
```

Desugaring notations

Coq offers a rich set of features to manage the increasing complexity of the objects we work with, such as coercions and notations. However, their heavy usage can make for quite overwhelming syntax. It is often instructive to "turn off" those features to get a more elementary picture of things, using the following commands:

- `Unset Printing Notations` (undo with `Set Printing Notations`)
- `Set Printing Coercions` (undo with `Unset Printing Coercions`)
- `Set Printing All` (undo with `Unset Printing All`)

These commands can also be used in the middle of a proof, to elaborate the current goal and context.

```
Unset Printing Notations.
Print fact_in_coq.
(* ===>
   fact_in_coq =
   CSeq (CAss Z X)
        (CSeq (CAss Y (S O))
              (CWhile (BNot (BEq Z O))
                      (CSeq (CAss Y (AMult Y Z))
                            (CAss Z (AMinus Z (S O)))))))
        : com *)
Set Printing Notations.

Set Printing Coercions.
Print fact_in_coq.
(* ===>
  fact_in_coq =
  <{ Z := (AId X);
     Y := (ANum 1);
     while ~ (AId Z) = (ANum 0) do
       Y := (AId Y) * (AId Z);
       Z := (AId Z) - (ANum 1)
     end }>
       : com *)
Unset Printing Coercions.
```

The `Locate` command

Finding notations

When faced with unknown notation, use `Locate` with a *string* containing one of its symbols to see its possible interpretations.

```
Locate "&&".
(* ===>
    Notation
      "x && y" := BAnd x y (default interpretation)
      "x && y" := andb x y : bool_scope (default interpretation)
*)
Locate ";".
(* ===>
    Notation
      "x '↦' v ';' m" := update m x v (default interpretation)
      "x ; y" := CSeq x y : com_scope (default interpretation)
      "x '!->' v ';' m" := t_update m x v (default interpretation)
      " x ; y ; .. ; z " := cons x (cons y .. (cons z nil) ..) : list_scope
      (default interpretation) *)

Locate "while".
(* ===>
    Notation
      "'while' x 'do' y 'end'" := CWhile x y : com_scope (default interpretation)
      "'_' '!->' v" := t_empty v (default interpretation)
*)
```

Finding identifiers

When used with an identifier, the command `Locate` prints the full path to every value in scope with the same name. This is useful to troubleshoot problems due to variable shadowing.

```
Locate aexp.
(* ===>
     Inductive LF.Imp.aexp
     Inductive LF.Imp.AExp.aexp
       (shorter name to refer to it in current context is AExp.aexp)
     Inductive LF.Imp.aevalR_division.aexp
       (shorter name to refer to it in current context is aevalR_division.aexp)
     Inductive LF.Imp.aevalR_extended.aexp
       (shorter name to refer to it in current context is aevalR_extended.aexp)
*)
```

More Examples

Assignment:

```
Definition plus2 : com :=
  <{ X := X + 2 }>.

Definition XtimesYinZ : com :=
  <{ Z := X × Y }>.

Definition subtract_slowly_body : com :=
  <{ Z := Z - 1 ;
     X := X - 1 }>.
```

Loops

```
Definition subtract_slowly : com :=
  <{ while ¬(X = 0) do
       subtract_slowly_body
     end }>.

Definition subtract_3_from_5_slowly : com :=
  <{ X := 3 ;
     Z := 5 ;
     subtract_slowly }>.
```

An infinite loop:

```
Definition loop : com :=
  <{ while true do
       skip
     end }>.
```

Evaluating Commands

Next we need to define what it means to evaluate an Imp command. The fact that `while` loops don't necessarily terminate makes defining an evaluation function tricky...

Evaluation as a Function (Failed Attempt)

Here's an attempt at defining an evaluation function for commands, omitting the `while` case.

The following declaration is needed to be able to use the notations in match patterns.

```
Fixpoint ceval_fun_no_while (st : state) (c : com) : state :=
  match c with
    | <{ skip }> ⇒
        st
    | <{ x := a }> ⇒
        (x !-> (aeval st a) ; st)
    | <{ c1 ; c2 }> ⇒
        let st' := ceval_fun_no_while st c1 in
        ceval_fun_no_while st' c2
    | <{ if b then c1 else c2 end}> ⇒
        if (beval st b)
          then ceval_fun_no_while st c1
          else ceval_fun_no_while st c2
    | <{ while b do c end }> ⇒
        st (* bogus *)
  end.
```

In a traditional functional programming language like OCaml or Haskell we could add the `while` case as follows:

```
Fixpoint ceval_fun (st : state) (c : com) : state :=
  match c with
    ...
    | while b do c end =>
        if (beval st b)
          then ceval_fun st (c ; while b do c end)
          else st
  end.
```

Coq doesn't accept such a definition ("Error: Cannot guess decreasing argument of fix") because the function we want to define is not guaranteed to terminate. Indeed, it *doesn't* always terminate: for example, the full version of the `ceval_fun` function applied to the `loop` program above would never terminate. Since Coq is not just a functional programming language but also a consistent logic, any potentially non-terminating function needs to be rejected. Here is an (invalid!) program showing what would go wrong if Coq allowed non-terminating recursive functions:

```
Fixpoint loop_false (n : nat) : False := loop_false n.
```

That is, propositions like `False` would become provable (`loop_false 0` would be a proof of `False`), which would be a disaster for Coq's logical consistency.

Thus, because it doesn't terminate on all inputs, of `ceval_fun` cannot be written in Coq -- at least not without additional tricks and workarounds (see chapter ImpCEvalFun if you're curious about what those might be).

Evaluation as a Relation

Here's a better way: define `ceval` as a *relation* rather than a *function* -- i.e., define it in `Prop` instead of `Type`, as we did for `aevalR` above.

This is an important change. Besides freeing us from awkward workarounds, it gives us a lot more flexibility in the definition. For example, if we add nondeterministic features like `any` to the language, we want the definition of evaluation to be nondeterministic -- i.e., not only will it not be total, it will not even be a function!

We'll use the notation `st =[ c ]=> st'` for the `ceval` relation: `st =[ c ]=> st'` means that executing program `c` in a starting state `st` results in an ending state `st'`. This can be pronounced "`c` takes state `st` to `st'`".

Operational Semantics

Here is an informal definition of evaluation, presented as inference rules for readability:

$$\frac{}{\texttt{st =[skip]=> st}}\ \text{(E\_Skip)}$$

$$\frac{\texttt{aeval st a = n}}{\texttt{st =[x := a]=> (x !-> n ; st)}}\ \text{(E\_Ass)}$$

$$\frac{\texttt{st =[c1]=> st'} \quad \texttt{st' =[c2]=> st''}}{\texttt{st =[c1;c2]=> st''}}\ \text{(E\_Seq)}$$

$$\frac{\texttt{beval st b = true} \quad \texttt{st =[c1]=> st'}}{\texttt{st =[if b then c1 else c2 end]=> st'}}\ \text{(E\_IfTrue)}$$

$$\frac{\texttt{beval st b = false} \quad \texttt{st =[c2]=> st'}}{\texttt{st =[if b then c1 else c2 end]=> st'}}\ \text{(E\_IfFalse)}$$

$$\frac{\texttt{beval st b = false}}{\texttt{st =[while b do c end]=> st}}\ \text{(E\_WhileFalse)}$$

$$\frac{\texttt{beval st b = true} \quad \texttt{st =[c]=> st'} \quad \texttt{st' =[while b do c end]=> st''}}{\texttt{st =[while b do c end]=> st''}}\ \text{(E\_WhileTrue)}$$

Here is the formal definition. Make sure you understand how it corresponds to the inference rules.

```
Reserved Notation
         "st '=[' c ']=>' st'"
         (at level 40, c custom com at level 99,
          st constr, st' constr at next level).

Inductive ceval : com → state → state → Prop :=
  | E_Skip : ∀ st,
      st =[ skip ]=> st
  | E_Ass : ∀ st a n x,
      aeval st a = n →
```

```
      st =[ x := a ]=> (x !-> n ; st)
  | E_Seq : ∀ c1 c2 st st' st'',
      st =[ c1 ]=> st' →
      st' =[ c2 ]=> st'' →
      st =[ c1 ; c2 ]=> st''
  | E_IfTrue : ∀ st st' b c1 c2,
      beval st b = true →
      st =[ c1 ]=> st' →
      st =[ if b then c1 else c2 end]=> st'
  | E_IfFalse : ∀ st st' b c1 c2,
      beval st b = false →
      st =[ c2 ]=> st' →
      st =[ if b then c1 else c2 end]=> st'
  | E_WhileFalse : ∀ b st c,
      beval st b = false →
      st =[ while b do c end ]=> st
  | E_WhileTrue : ∀ st st' st'' b c,
      beval st b = true →
      st =[ c ]=> st' →
      st' =[ while b do c end ]=> st'' →
      st =[ while b do c end ]=> st''

  where "st =[ c ]=> st'" := (ceval c st st').
```

The cost of defining evaluation as a relation instead of a function is that we now need to construct *proofs* that some program evaluates to some result state, rather than just letting Coq's computation mechanism do it for us.

```
Example ceval_example1:
  empty_st =[
     X := 2;
     if (X ≤ 1)
       then Y := 3
       else Z := 4
     end
  ]=> (Z !-> 4 ; X !-> 2).
Proof.
  (* We must supply the intermediate state *)
  apply E_Seq with (X !-> 2).
  - (* assignment command *)
    apply E_Ass. reflexivity.
  - (* if command *)
    apply E_IfFalse.
    reflexivity.
    apply E_Ass. reflexivity.
Qed.
```

Exercise: 2 stars, standard (ceval_example2)

```
Example ceval_example2:
  empty_st =[
    X := 0;
    Y := 1;
    Z := 2
  ]=> (Z !-> 2 ; Y !-> 1 ; X !-> 0).
Proof.
  (* FILL IN HERE *) Admitted.
□

Set Printing Implicit.
Check @ceval_example2.
```

Exercise: 3 stars, standard, optional (pup_to_n)

Write an Imp program that sums the numbers from `1` to `X` (inclusive: `1 + 2 + ... + X`) in the variable `Y`. Your program should update the state as shown in theorem `pup_to_2_ceval`, which you can reverse-engineer to discover the program you should write. The proof of that theorem will be somewhat lengthy.

```
Definition pup_to_n : com
  (* REPLACE THIS LINE WITH ":= _your_definition_ ." *). Admitted.

Theorem pup_to_2_ceval :
  (X !-> 2) =[
    pup_to_n
  ]=> (X !-> 0 ; Y !-> 3 ; X !-> 1 ; Y !-> 2 ; Y !-> 0 ; X !-> 2).
Proof.
  (* FILL IN HERE *) Admitted.
□
```

Determinism of Evaluation

Changing from a computational to a relational definition of evaluation is a good move because it frees us from the artificial requirement that evaluation should be a total function. But it also raises a question: Is the second definition of evaluation really a partial *function*? Or is it possible that, beginning from the same state `st`, we could evaluate some command `c` in different ways to reach two different output states `st'` and `st''`?

In fact, this cannot happen: `ceval` *is* a partial function:

```
Theorem ceval_deterministic: ∀ c st st1 st2,
     st =[ c ]=> st1 →
     st =[ c ]=> st2 →
     st1 = st2.
```

Reasoning About Imp Programs

We'll get deeper into more systematic and powerful techniques for reasoning about Imp programs in *Programming Language Foundations*, but we can get some distance just working with the bare definitions. This section explores some examples.

```
Theorem plus2_spec : ∀ st n st',
  st X = n →
  st =[ plus2 ]=> st' →
  st' X = n + 2.
Proof.
  intros st n st' HX Heval.
```

Inverting `Heval` essentially forces Coq to expand one step of the `ceval` computation -- in this case revealing that `st'` must be `st` extended with the new value of `X`, since `plus2` is an assignment.

```
  inversion Heval. subst. clear Heval. simpl.
  apply t_update_eq. Qed.
```

Exercise: 3 stars, standard, optional (XtimesYinZ_spec)

State and prove a specification of `XtimesYinZ`.

```
(* FILL IN HERE *)

(* Do not modify the following line: *)
Definition manual_grade_for_XtimesYinZ_spec : option (nat×string) := None.
```
□

Exercise: 3 stars, standard, especially useful (loop_never_stops)

```
Theorem loop_never_stops : ∀ st st',
  ~(st =[ loop ]=> st').
Proof.
  intros st st' contra. unfold loop in contra.
  remember <{ while true do skip end }> as loopdef
           eqn:Heqloopdef.
```

Proceed by induction on the assumed derivation showing that `loopdef` terminates. Most of the cases are immediately contradictory (and so can be solved in one step with `discriminate`).

```
  (* FILL IN HERE *) Admitted.
```
□

Exercise: 3 stars, standard (no_whiles_eqv)

Consider the following function:

```
Fixpoint no_whiles (c : com) : bool :=
  match c with
  | <{ skip }> ⇒
      true
  | <{ _ := _ }> ⇒
      true
  | <{ c1 ; c2 }> ⇒
      andb (no_whiles c1) (no_whiles c2)
  | <{ if _ then ct else cf end }> ⇒
      andb (no_whiles ct) (no_whiles cf)
  | <{ while _ do _ end }> ⇒
      false
  end.
```

This predicate yields `true` just on programs that have no while loops. Using `Inductive`, write a property `no_whilesR` such that `no_whilesR c` is provable exactly when `c` is a program with no while loops. Then prove its equivalence with `no_whiles`.

```
Inductive no_whilesR: com → Prop :=
 (* FILL IN HERE *)
.

Theorem no_whiles_eqv:
   ∀ c, no_whiles c = true ↔ no_whilesR c.
Proof.
  (* FILL IN HERE *) Admitted.
```
□

Exercise: 4 stars, standard (no_whiles_terminating)

Imp programs that don't involve while loops always terminate. State and prove a theorem `no_whiles_terminating` that says this. Use either `no_whiles` or `no_whilesR`, as you prefer.

```
(* FILL IN HERE *)

(* Do not modify the following line: *)
Definition manual_grade_for_no_whiles_terminating : option (nat×string) := None.
```
□

Additional Exercises

Exercise: 3 stars, standard (stack_compiler)

Old HP Calculators, programming languages like Forth and Postscript, and abstract machines like the Java Virtual Machine all evaluate arithmetic expressions using a *stack*. For instance, the expression

```
(2*3)+(3*(4-2))
```

would be written as

```
2 3 * 3 4 2 - * +
```

and evaluated like this (where we show the program being evaluated on the right and the contents of the stack on the left):

```
[ ]            |    2 3 * 3 4 2 - * +
[2]            |    3 * 3 4 2 - * +
[3, 2]         |    * 3 4 2 - * +
[6]            |    3 4 2 - * +
[3, 6]         |    4 2 - * +
[4, 3, 6]      |    2 - * +
[2, 4, 3, 6]   |    - * +
[2, 3, 6]      |    * +
[6, 6]         |    +
[12]           |
```

The goal of this exercise is to write a small compiler that translates `aexp`s into stack machine instructions.

The instruction set for our stack language will consist of the following instructions:

- `SPush n`: Push the number `n` on the stack.
- `SLoad x`: Load the identifier `x` from the store and push it on the stack
- `SPlus`: Pop the two top numbers from the stack, add them, and push the result onto the stack.
- `SMinus`: Similar, but subtract the first number from the second.
- `SMult`: Similar, but multiply.

```
Inductive sinstr : Type :=
| SPush (n : nat)
| SLoad (x : string)
| SPlus
| SMinus
| SMult.
```

Write a function to evaluate programs in the stack language. It should take as input a state, a stack represented as a list of numbers (top stack item is the head of the list), and a program represented as a list of instructions,

and it should return the stack after executing the program. Test your function on the examples below.

Note that it is unspecified what to do when encountering an `SPlus`, `SMinus`, or `SMult` instruction if the stack contains fewer than two elements. In a sense, it is immaterial what we do, since a correct compiler will never emit such a malformed program. But for sake of later exercises, it would be best to skip the offending instruction and continue with the next one.

```
Fixpoint s_execute (st : state) (stack : list nat)
                   (prog : list sinstr)
                 : list nat
  (* REPLACE THIS LINE WITH ":= _your_definition_ ." *). Admitted.

Check s_execute.

Example s_execute1 :
     s_execute empty_st []
       [SPush 5; SPush 3; SPush 1; SMinus]
   = [2; 5].
(* FILL IN HERE *) Admitted.

Example s_execute2 :
     s_execute (X !-> 3) [3;4]
       [SPush 4; SLoad X; SMult; SPlus]
   = [15; 4].
(* FILL IN HERE *) Admitted.
```

Next, write a function that compiles an `aexp` into a stack machine program. The effect of running the program should be the same as pushing the value of the expression on the stack.

```
Fixpoint s_compile (e : aexp) : list sinstr
  (* REPLACE THIS LINE WITH ":= _your_definition_ ." *). Admitted.
```

After you've defined `s_compile`, prove the following to test that it works.

```
Example s_compile1 :
  s_compile <{ X - (2 * Y) }>
  = [SLoad X; SPush 2; SLoad Y; SMult; SMinus].
(* FILL IN HERE *) Admitted.
□
```

Exercise: 3 stars, standard (execute_app)

Execution can be decomposed in the following sense: executing stack program p_1 `++` p_2 is the same as executing p_1, taking the resulting stack, and executing p_2 from that stack. Prove that fact.

```
Theorem execute_app : ∀ st p1 p2 stack,
    s_execute st stack (p1 ++ p2) = s_execute st (s_execute st stack p1) p2.
Proof.
  (* FILL IN HERE *) Admitted.
□
```

Exercise: 3 stars, standard (stack_compiler_correct)

Now we'll prove the correctness of the compiler implemented in the previous exercise. Begin by proving the following lemma. If it becomes difficult, consider whether your implementation of `s_execute` or `s_compile` could be simplified.

```
Lemma s_compile_correct_aux : ∀ st e stack,
  s_execute st stack (s_compile e) = aeval st e :: stack.
Proof.
  (* FILL IN HERE *) Admitted.
```

The main theorem should be a very easy corollary of that lemma.

```
Theorem s_compile_correct : ∀ (st : state) (e : aexp),
  s_execute st [] (s_compile e) = [ aeval st e ].
Proof.
  (* FILL IN HERE *) Admitted.
□
```

Exercise: 3 stars, standard, optional (short_circuit)

Most modern programming languages use a "short-circuit" evaluation rule for boolean `and`: to evaluate `BAnd` b_1 b_2, first evaluate b_1. If it evaluates to `false`, then the entire `BAnd` expression evaluates to `false` immediately, without evaluating b_2. Otherwise, b_2 is evaluated to determine the result of the `BAnd` expression.

Write an alternate version of `beval` that performs short-circuit evaluation of `BAnd` in this manner, and prove that it is equivalent to `beval`. (N.b. This is only true because expression evaluation in Imp is rather simple. In a bigger language where evaluating an expression might diverge, the short-circuiting `BAnd` would *not* be equivalent to the original, since it would make more programs terminate.)

```
(* FILL IN HERE *)
□

Module BreakImp.
```

Exercise: 4 stars, advanced (break_imp)

Imperative languages like C and Java often include a `break` or similar statement for interrupting the execution of loops. In this exercise we consider how to add `break` to Imp. First, we need to enrich the language of commands with an additional case.

```
Inductive com : Type :=
  | CSkip
  | CBreak (* <--- NEW *)
  | CAss (x : string) (a : aexp)
  | CSeq (c1 c2 : com)
  | CIf (b : bexp) (c1 c2 : com)
  | CWhile (b : bexp) (c : com).

Notation "'break'" := CBreak (in custom com at level 0).
Notation "'skip'" :=
         CSkip (in custom com at level 0) : com_scope.
Notation "x := y" :=
         (CAss x y)
            (in custom com at level 0, x constr at level 0,
             y at level 85, no associativity) : com_scope.
Notation "x ; y" :=
         (CSeq x y)
           (in custom com at level 90, right associativity) : com_scope.
```

```
Notation "'if' x 'then' y 'else' z 'end'" :=
         (CIf x y z)
           (in custom com at level 89, x at level 99,
            y at level 99, z at level 99) : com_scope.
Notation "'while' x 'do' y 'end'" :=
         (CWhile x y)
            (in custom com at level 89, x at level 99, y at level 99) : com_scope.
```

Next, we need to define the behavior of `break`. Informally, whenever `break` is executed in a sequence of commands, it stops the execution of that sequence and signals that the innermost enclosing loop should terminate. (If there aren't any enclosing loops, then the whole program simply terminates.) The final state should be the same as the one in which the `break` statement was executed.

One important point is what to do when there are multiple loops enclosing a given `break`. In those cases, `break` should only terminate the *innermost* loop. Thus, after executing the following...

```
X := 0;
Y := 1;
while ~(0 = Y) do
  while true do
    break
  end;
  X := 1;
  Y := Y - 1
end
```

... the value of `X` should be `1`, and not `0`.

One way of expressing this behavior is to add another parameter to the evaluation relation that specifies whether evaluation of a command executes a `break` statement:

```
Inductive result : Type :=
  | SContinue
  | SBreak.

Reserved Notation "st '=[' c ']=>' st' '/' s"
     (at level 40, c custom com at level 99, st' constr at next level).
```

Intuitively, `st =[ c ]=> st' / s` means that, if `c` is started in state `st`, then it terminates in state `st'` and either signals that the innermost surrounding loop (or the whole program) should exit immediately (`s = SBreak`) or that execution should continue normally (`s = SContinue`).

The definition of the "`st =[ c ]=> st' / s`" relation is very similar to the one we gave above for the regular evaluation relation (`st =[ c ]=> st'`) -- we just need to handle the termination signals appropriately:

- If the command is `skip`, then the state doesn't change and execution of any enclosing loop can continue normally.
- If the command is `break`, the state stays unchanged but we signal a `SBreak`.
- If the command is an assignment, then we update the binding for that variable in the state accordingly and signal that execution can continue normally.
- If the command is of the form `if b then` c_1 `else` c_2 `end`, then the state is updated as in the original semantics of Imp, except that we also propagate the signal from the execution of whichever branch was taken.
- If the command is a sequence c_1 `;` c_2, we first execute c_1. If this yields a `SBreak`, we skip the execution of c_2 and propagate the `SBreak` signal to the surrounding context; the resulting state is the same as the one obtained by executing c_1 alone. Otherwise, we execute c_2 on the state obtained after executing c_1, and propagate the signal generated there.
- Finally, for a loop of the form `while b do c end`, the semantics is almost the same as before. The only difference is that, when `b` evaluates to true, we execute `c` and check the signal that it raises. If that signal is `SContinue`, then the execution proceeds as in the original semantics. Otherwise, we stop the execution of the loop, and the resulting state is the same as the one resulting from the execution of the current iteration. In either case, since `break` only terminates the innermost loop, `while` signals `SContinue`.

Based on the above description, complete the definition of the `ceval` relation.

```
(* FILL IN HERE *)

Inductive ceval : com → state → result → state → Prop :=
  | E_Skip : ∀ st,
      st =[ CSkip ]=> st / SContinue
  (* FILL IN HERE *)

  where "st '=[' c ']=>' st' '/' s" := (ceval c st s st').
```

Now prove the following properties of your definition of `ceval`:

```
Theorem break_ignore : ∀ c st st' s,
     st =[ break; c ]=> st' / s →
     st = st'.
Proof.
  (* FILL IN HERE *) Admitted.

Theorem while_continue : ∀ b c st st' s,
  st =[ while b do c end ]=> st' / s →
  s = SContinue.
Proof.
  (* FILL IN HERE *) Admitted.

Theorem while_stops_on_break : ∀ b c st st',
  beval st b = true →
  st =[ c ]=> st' / SBreak →
  st =[ while b do c end ]=> st' / SContinue.
Proof.
  (* FILL IN HERE *) Admitted.
□
```

Exercise: 3 stars, advanced, optional (while_break_true)

```
Theorem while_break_true : ∀ b c st st',
  st =[ while b do c end ]=> st' / SContinue →
  beval st' b = true →
  ∃ st'', st'' =[ c ]=> st' / SBreak.
Proof.
(* FILL IN HERE *) Admitted.
□
```

Exercise: 4 stars, advanced, optional (ceval_deterministic)

```
Theorem ceval_deterministic: ∀ (c:com) st st1 st2 s1 s2,
     st =[ c ]=> st1 / s1 →
     st =[ c ]=> st2 / s2 →
     st1 = st2 ∧ s1 = s2.
Proof.
  (* FILL IN HERE *) Admitted.
□
End BreakImp.
```

Exercise: 4 stars, standard, optional (add_for_loop)

Add C-style `for` loops to the language of commands, update the `ceval` definition to define the semantics of `for` loops, and add cases for `for` loops as needed so that all the proofs in this file are accepted by Coq.

A `for` loop should be parameterized by (a) a statement executed initially, (b) a test that is run on each iteration of the loop to determine whether the loop should continue, (c) a statement executed at the end of each loop iteration, and (d) a statement that makes up the body of the loop. (You don't need to worry about making up a concrete Notation for `for` loops, but feel free to play with this too if you like.)

```
(* FILL IN HERE *)
□

(* 2020-09-09 20:51 *)
```