Operational and Denotational Semantics

Please turn in by April 5, 2011 (-1 point penalty per day late)

Solution.

We consider an enriched, typed λ-calculus with constants for arithmetic expressions and recursion. Note that the essential question is question 9. This is the one that takes the longest to answer, and the one that will really tell me whether you understand (variants of) techniques we have seen in the λ-calculus.

The *types* are $\sigma, \tau ::= \mathtt{Nat} \mid \sigma \to \tau$. All the terms in the language come with explicit types. In particular, we assume an infinite, countable set of variables of each type τ, and write x_τ for a variable of type τ.

The terms t of type τ (in short, $t : \tau$) are defined by induction on their size by :

- every variable x_τ is of type τ ;
- if $N : \tau$, then $\lambda x_\sigma \cdot N$ is a term of type $\sigma \to \tau$;
- if $M : \sigma \to \tau$ and $N : \sigma$, then MN is a term of type τ ;
- for each $n \in \mathbb{N}$, there is a distinct constant $\underline{n} : \mathtt{Nat}$;
- there are distinct constants $\mathtt{pred} : \mathtt{Nat} \to \mathtt{Nat}$ (subtract one), $\mathtt{succ} : \mathtt{Nat}$ (add one), $\mathtt{ifz}_\tau : \mathtt{Nat} \to \tau \to \tau \to \tau$ (test if first argument equals 0), and $Y_\tau : (\tau \to \tau) \to \tau$ (fixpoint, recursion).

As in the λ-calculus, the terms are understood up to α-renaming. This takes the special form that x_σ can be replaced by any fresh variable y_σ of the *same* type σ in $\lambda x_\sigma \cdot t$. We drop type indices whenever they are irrelevant or can be reconstructed from context.

We define its semantics not through reduction, but by building a machine directly.

The *contexts* are defined by the grammar $E := \_ \mid EN \mid \mathtt{succ}\, E \mid \mathtt{pred}\, E \mid \mathtt{ifz}\ E\ N\ P$, where N, P denote terms. . We see contexts as particular terms, with a unique occurrence of a specific variable $\_$ that does not occur in any term, called the *hole*. A context E is of type $\sigma \vdash \tau$ when E is of type τ, assuming the hole $\_$ of type σ. $E[M]$ denotes the replacement of the hole by M (of type σ).

Our machine is a transition system whose configurations are pairs $E \cdot M$. Intuitively, in such a configuration, the machine is in the process of evaluating $E[M]$, and the focus is currently on the subterm M.

The machine rules come into two groups. The first form the *redex discovery* rules. E.g., in $(DApp)$, the machine tries to evaluate MN, and proceeds by pushing the argument N into the context and focusing on the function part M.

$$\begin{array}{cccc} (DApp) & E \cdot MN \to E[\_N] \cdot M & (DIf) & E[\_MNP] \cdot \texttt{ifz} \to E[\texttt{ifz}\ \_\ N\ P] \cdot M \\ (DPred) & E[\_N] \cdot \texttt{pred} \to E[\texttt{pred}\ \_] \cdot N & (DSucc) & E[\_N] \cdot \texttt{succ} \to E[\texttt{succ}\ \_] \cdot N \end{array}$$

The second group of rules *computes* :

$$\begin{array}{cccc} (\beta) & E[\_N] \cdot \lambda x \cdot P \to E \cdot P[x := N] & (Y) & E[\_N] \cdot Y \to E \cdot N(YN) \\ (\texttt{pred}) & E[\texttt{pred}\ \_] \cdot \underline{n+1} \to E \cdot \underline{n} & (\texttt{succ}) & E[\texttt{succ}\ \_] \cdot \underline{n} \to E \cdot \underline{n+1} \\ (\texttt{ifz}0) & E[\texttt{ifz}\ \_\ N\ P] \cdot \underline{0} \to E \cdot N & (\texttt{ifz}1) & E[\texttt{ifz}\ \_\ N\ P] \cdot \underline{n+1} \to E \cdot P \end{array}$$

We do *not* take the closure of $\to$ under contexts, whatever this may mean. The relation $\to$ is entirely specified by the rules above.

We also consider a *denotational semantics* of the above terms. First, we define the cpo $[\![\tau]\!]$ of all *values* of type τ :

- $[\![\texttt{Nat}]\!]$ is $\mathbb{N}_\perp$, the set of all natural numbers plus an added, so-called *bottom* element $\perp$. These are ordered by $m \leq n$ iff $m = \perp$ or $m = n$. (Think as all element of $\mathbb{N}$ being incomparable and above $\perp$.)
- $[\![\sigma \to \tau]\!]$ is the dcpo $[[\![\sigma]\!] \to [\![\tau]\!]]$ of all continuous maps from $[\![\sigma]\!]$ to $[\![\tau]\!]$. They are ordered by $f \leq g$ iff $f(x) \leq g(x)$ in $[\![\tau]\!]$ for every $x \in [\![\sigma]\!]$.

1. Show that every term t has exactly one type.

   This is by induction on the size of t, using the fact that every term has at least one type by definition, and conversely that the type is determined from a unique typing rule. E.g., if our term is MN, then M has a unique type, N has a unique type, and since MN has a type at all, it must be obtained by the rule "if $M : \sigma \to \tau$ and $N : \sigma$ then MN is a term of type τ", which determines τ uniquely. If our term is $\lambda x_\sigma \cdot N$, then N has a unique type τ, and therefore the unique type of $\lambda x_\sigma \cdot N$ is $\sigma \to \tau$. This is the only interesting case, and justifies why we explicitly decorate the variable x_σ with its type. Finally, the types of variables and constants are uniquely determined.

2. Show that $[\![\tau]\!]$ has a least element $\perp_\tau$, for every type τ. By abuse of language, we shall write $\perp$ instead of $\perp_\tau$, and call it "bottom". It is useful to think of $\perp$ as non-termination.

   By induction on τ. $\mathbb{N}_\perp$ has $\perp$ as its least element, and if $\perp_\tau$ is the least element of $[\![\tau]\!]$, then the constant map with value $\perp_\tau$ is the bottom element of $[\![\sigma \to \tau]\!]$.

Then we define the semantics $[\![t]\!]\,\rho$ of terms $t : \tau$ as values in $[\![\tau]\!]$ in *environments* ρ mapping each variable x_σ to an element of $[\![\sigma]\!]$, by :

- $[\![x_\sigma]\!]\,\rho = \rho(x_\sigma)$;
- $[\![MN]\!]\,\rho = [\![M]\!]\,\rho([\![N]\!]\,\rho)$;
- $[\![\lambda x_\sigma \cdot N]\!]\,\rho$ is the function that maps each $v \in [\![\sigma]\!]$ to $[\![N]\!]\,(\rho[x_\sigma := v])$;
- $[\![\underline{n}]\!]\,\rho = n$, for every $n \in \mathbb{N}$;

- $[\![\texttt{pred}]\!]\,\rho$ is the map that sends $n+1$ to $n \in \mathbb{N}$, and 0 and $\bot$ to $\bot$;
- $[\![\texttt{succ}]\!]\,\rho$ is the map that sends $n \in \mathbb{N}$ to $n+1$, and $\bot$ to $\bot$;
- $[\![\texttt{ifz}_\tau]\!]\,\rho$ is the map that sends u, v, w to $\bot$ if $u = \bot$, to v if $u = 0$, and to w if $u \neq 0, \bot$;
- $[\![Y_\tau]\!]\,\rho$ is the map that sends $f \in [[\![\tau]\!] \to [\![\tau]\!]]$ to $\sup_{n\in\mathbb{N}} f^n(\bot_\tau)$.

3. Given any continuous map $f \in [[\![\tau]\!] \to [\![\tau]\!]]$, show that $lfp(f) = \sup_{n\in\mathbb{N}} f^n(\bot_\tau)$ exists in $[\![\tau]\!]$, and is the *least fixpoint* of f. A fixpoint of f is an element v such that $f(v) = v$. It is least iff $v \leq w$ for every other fixpoint w. (This is meant to explain the definition of $[\![Y_\tau]\!]\,\rho$.)

   We first check that $(f^n(\bot_\tau))_{n\in\mathbb{N}}$ is a chain, i.e., $f^0(\bot_\tau) \leq f^1(\bot_\tau) \leq \ldots \leq f^n(\bot_\tau) \leq \ldots$ It is enough to check that $f^n(\bot_\tau) \leq f^{n+1}(\bot_\tau)$ for every $n \in \mathbb{N}$, and this is done by induction on n. If $n = 0$, this is because $f^0(\bot_\tau) = \bot_\tau$ is least. Otherwise, $f^n(\bot_\tau) = f(f^{n-1}(\bot_\tau)) \leq f(f^n(\bot_\tau)) = f^{n+1}(\bot_\tau)$ by induction hypothesis and the fact that f is monotonic.

   Now $lfp(f)$ is a fixpoint : $f(lfp(f)) = f(\sup_{n\in\mathbb{N}} f^n(\bot_\tau) = \sup_{n\in\mathbb{N}} f^{n+1}(\bot_\tau)$, because f is continuous and $(f^n(\bot_\tau))_{n\in\mathbb{N}}$ is a chain; we conclude because $\sup_{n\in\mathbb{N}} f^n(\bot_\tau) = \sup(f^0(\bot_\tau), \sup_{n\in\mathbb{N}} f^{n+1}(\bot_\tau)) = \sup(\bot_\tau, \sup_{n\in\mathbb{N}} f^{n+1}(\bot_\tau)) = \sup_{n\in\mathbb{N}} f^{n+1}(\bot_\tau)$.

   We claim that $lfp(f)$ is the least one. Assume x is another fixpoint. By induction on n, $f^n(\bot_\tau) \leq x$: this is clear if $n = 0$, since $\bot_\tau$ is least, otherwise $f^{n+1}(\bot_\tau) = f(f^n(\bot_\tau)) \leq f(x)$ (by induction hypothesis, and since f is monotonic) $= x$ (since x is a fixpoint). Taking sups on each side, $lfp(f) \leq x$.

4. Establish *soundness* : if $E \cdot M \to^* \_ \cdot \underline{n}$, then $[\![E[M]]\!]\,\rho = n$, for every $n \in \mathbb{N}$, and every environment ρ.

   We first show that : (1) if $E \cdot M \to E' \cdot M'$, then $[\![E[M]]\!]\,\rho = [\![E'[M']]\!]\,\rho$. By induction on the number of $\to$ steps, it will follow that if $E \cdot M \to^* \_ \cdot \underline{n}$, then $[\![E[M]]\!]\,\rho = [\![\_[\underline{n}]]\!]\,\rho = n$.

   Claim (1) is obvious in the cases of the rules $(DApp)$, (DIf), $(DPred)$ and $(DSucc)$, since in these cases $E[M] = E'[M']$.

   For the other rules, we note that for any configuration $E'' \cdot M''$, $[\![E'' \cdot M'']\!]\,\rho = [\![E'']\!]\,(\rho[\_ \mapsto [\![M'']\!]\,\rho])$. This is a form of the substitution lemma we have seen in the lectures, and is proved by induction on the size of E''.

   It remains to show that :

   (β) $[\![(\lambda x \cdot P)N]\!]\,\rho = [\![P[x := N]]\!]\,\rho$ *: the left-hand side is $(v \mapsto [\![P]\!]\,(\rho[x := v]))([\![N]\!]\,\rho) = [\![P]\!]\,(\rho[x := [\![N]\!]\,\rho])$, which is equal to the right-hand side by the substitution lemma.*

   (Y) $[\![YN]\!]\,\rho = [\![N(YN)]\!]\,\rho$ *: the left-hand side is $lfp(f)$, where $f = [\![N]\!]\,\rho$, while the right-hand side is $f(lfp(f))$. These two are equal because $lfp(f)$ is a fixpoint of f, as we have seen.*

   $(\texttt{pred})$ $[\![\texttt{pred}\,\underline{n+1}]\!]\,\rho = [\![\underline{n}]\!]\,\rho$ *: both sides equal n.*

   $(\texttt{succ})$ $[\![\texttt{succ}\,\underline{n}]\!]\,\rho = [\![\underline{n+1}]\!]\,\rho$ *: both sides equals $n+1$.*

(ifz0) $[\![\texttt{ifz}\ \underline{0}\ N\ P]\!]\,\rho = [\![N]\!]\,\rho$ *: obvious.*

(ifz1) $[\![\texttt{ifz}\ \underline{n+1}\ N\ P]\!]\,\rho = [\![P]\!]\,\rho$ *: obvious.*

The rest of the questions aim at establishing the converse of soundness, a property known as *computational adequacy*. This is harder : notice in particular that computational adequacy entails that if $[\![E[M]]\!]\,\rho = n$ for every $n \in \mathbb{N}$, and every environment ρ, then $E \cdot M$ must terminate (on the configuration $\_ \cdot \underline{n}$).

We first show that we can only hope to prove computational adequacy in a limited setting. First, we only consider *ground configurations* : call a term *ground* iff it has no free variable, and a configuration $E \cdot M$ *ground* iff $E[M]$ is ground. Then $[\![E[M]]\!]\,\rho$ does not depend on ρ, and we shall write it $[\![E[M]]\!]$.

5. One might think of proving computational adequacy at every type τ, i.e., that if $E \cdot M$ is ground, and $[\![E[M]]\!]$ is a value $v \in [\![\tau]\!]$ (the same for every environment ρ), then $E \cdot M \to^* \_ \cdot M'$ for some canonical ground term $M' : \tau$ with $[\![M']\!] = v$. By "canonical", we mean that there is a unique canonical term M' such that $[\![M']\!] = v$. Show that this is hopeless : canonicality fails, at least for some type τ other than $\texttt{Nat}$.

   Take $E = \_$, $M_1 = \lambda x_\sigma \cdot \texttt{succ}\,\underline{1}$ and $M_2 = \lambda x_\sigma \cdot \underline{2}$. These two terms have the same value, namely the constant 2 function. Canonicality would imply that $\_ \cdot M_1$ and $\_ \cdot M_2$ would rewrite to the same $\_ \cdot M'$. But $\_ \cdot M_1$ and $\_ \cdot M_2$ do not rewrite at all.

Define $\precsim_\sigma$ on ground terms by $M \precsim_\sigma N$ iff for every context E of type $\sigma \vdash \texttt{Nat}$, if $E \cdot M \to^* \_ \cdot \underline{n}$ then $E \cdot N \to^* \_ \cdot \underline{n}$.

Extend $\precsim_\sigma$ to non-ground terms by $M \precsim_\sigma N$ iff $M\theta \precsim_\sigma N\theta$ for every well-typed substitution θ of ground terms for all variables in M and N. A substitution θ is *well-typed* iff $x_\sigma\theta$ is a term of type σ for every variable x_σ in its domain.

6. Show that :
   - $M[x_\sigma := N] \precsim_\tau (\lambda x_\sigma \cdot M)N$ whenever $M : \tau$, $N : \sigma$;
   - $M(YM) \precsim_\tau YM$ provided $M : \tau \to \tau$;
   - if $\underline{n} \precsim_{\texttt{Nat}} M$ then $\underline{n+1} \precsim_{\texttt{Nat}} \texttt{succ}\,M$;
   - if $\underline{n+1} \precsim_{\texttt{Nat}} M$ then $\underline{n} \precsim_{\texttt{Nat}} \texttt{pred}\,M$;
   - if $\underline{0} \precsim_{\texttt{Nat}} M$ then $N \precsim_\tau \texttt{ifz}\ M\ N\ P$ (where $N : \tau$, $P : \tau$),
   - if $\underline{n+1} \precsim_{\texttt{Nat}} M$ then $P \precsim_\tau \texttt{ifz}\ M\ N\ P$ (where $N : \tau$, $P : \tau$).

   We show the claims assuming each side of the inequalities ground. The general case follows by applying some well-typed substitution θ throughout.
   - *$M[x_\sigma := N] \precsim_\tau (\lambda x_\sigma \cdot M)N$: if $E \cdot M[x_\sigma := N] \to^* \_ \cdot \underline{n}$, then $E \cdot (\lambda x_\sigma \cdot M)N \to E[\_N] \cdot \lambda x_\sigma \cdot M$ (by $(DApp)$) $\to E \cdot M[x_\sigma := N]$ (by (β)) $\to^* \_ \cdot \underline{n}$ (by assumption).*
   - *$M(YM) \precsim_\tau YM$: similarly, $E \cdot YM \to E[\_M]Y \to E \cdot M(YM)$ by $(DApp)$ and (Y).*
   - *If $\underline{n+1} \precsim_{\texttt{Nat}} M$ then $\underline{n} \precsim_{\texttt{Nat}} \texttt{pred}\,M$. This is slightly different. Assume that $E \cdot \underline{n} \to^* \_ \cdot \underline{m}$ for some $m \in \mathbb{N}$. So $E[\texttt{pred}\,\_] \cdot \underline{n+1} \to E \cdot \underline{n}$ (by $(\texttt{pred})$) $\to^* \_ \cdot \underline{m}$. Since $\underline{n+1} \precsim_{\texttt{Nat}} M$, and using the context $E[\texttt{pred}\,\_]$, $E[\texttt{pred}\,\_] \cdot M \to^* \_ \cdot \underline{m}$. But then $E \cdot \texttt{pred}\,M \to E[\_M] \cdot \texttt{pred}$ (by $(DApp)$) $\to E[\texttt{pred}\,\_] \cdot M$ (by $(DPred)$) $\to^* \_ \cdot \underline{m}$.*

– *If* $\underline{n+1} \precsim_{\mathtt{Nat}} M$ *then* $\underline{n} \precsim_{\mathtt{Nat}} \mathtt{pred}\, M$. *Similar, using* $(\mathtt{succ})$ *and* $(DSucc)$ *instead.*
– *If* $\underline{0} \precsim_{\mathtt{Nat}} M$ *then* $N \precsim_\tau \mathtt{ifz}\ M\ N\ P$. *Assume* $E \cdot N \to^* \_ \cdot \underline{m}$, *and use the context* $E[\mathtt{ifz}\ \_\ N\ P]$. *Since* $\underline{0} \precsim_{\mathtt{Nat}} M$ *and* $E[\mathtt{ifz}\ \_\ N\ P] \cdot \underline{0} \to E \cdot N$ *(by* $(\mathtt{ifz}0)$*)* $\to^* \_ \cdot \underline{m}$, *we must have* $E[\mathtt{ifz}\ \_\ N\ P] \cdot M \to^* \_ \cdot \underline{m}$, *so* $E \cdot \mathtt{ifz}\ M\ N\ P \to E[\_P] \cdot \mathtt{ifz} MN \to E[\_NP] \cdot \mathtt{ifz} M \to E[\_MNP] \cdot \mathtt{ifz} \to E[\mathtt{ifz}\ \_\ N\ P] \cdot M \to E \cdot N \to^* \_ \cdot \underline{m}$, *using* $(DApp)$ *three times, then* (DIf).
– *If* $\underline{n+1} \precsim_{\mathtt{Nat}} M$ *then* $P \precsim_\tau \mathtt{ifz}\ M\ N\ P$. *Similar, using* $(\mathtt{ifz}1)$ *instead.*

The main tool in the proof of computational adequacy is the use of a so-called *logical relation*. This is a notion similar to the reducibility sets RED_τ defined in the lectures, except there are now binary relations, i.e., sets of pairs.

Here, a logical relation is a family of binary relations R_τ, indexed by types τ, between values in $[\![\tau]\!]$ and ground terms $M : \tau$. These are defined by induction on types as follows. For short, we say "for all $N\ R_\sigma\ v$" instead of "for every term $N : \sigma$, every value $v \in [\![\sigma]\!]$, if $N\ R_\sigma\ v$ then".
– $M\ R_{\mathtt{Nat}}\ u$ iff $u = \bot$, or u is a natural number n and $\underline{n} \precsim_{\mathtt{Nat}} M$.
– $M\ R_{\sigma\to\tau}\ f$ iff for all $N\ R_\sigma\ v$, $MN\ R_\tau\ f(v)$.

7. Given $M : \tau$, let MR_τ be the set $\{u \in [\![\tau]\!] \mid M\ R_\tau\ u\}$. Show that MR_τ is *Scott-closed*, i.e., both *downward closed* (if $u \leq v$ and $M\ R_\tau\ v$ then $M\ R_\tau\ u$) and stable under directed sups (if $(u_i)_{i\in I}$ is a directed family in $[\![\tau]\!]$, and $M\ R_\tau\ u_i$ for every $i \in I$, then $M\ R_\tau \sup_{i\in I} u_i$). Show also that MR_τ is non-empty, i.e., contains $\bot$.

   By induction on types. $MR_{\mathtt{Nat}}$ *is* $\{\bot\} \cup \{n \in \mathbb{N} \mid \underline{n} \precsim_{\mathtt{Nat}} M$, *so it contains* $\bot$ *and is downward closed (the only elements below* $n \in \mathbb{N}$ *are* n *and* $\bot$*). It is also closed under directed sups because every non-empty subset* A *of* $\mathbb{N}_\bot$ *is : either* $A = \{\bot\}$ *and this is clear, or* A *contains some* $n \in \mathbb{N}$, *then every* $m \in A$ *is below some element above both* n *and* m *by directedness, which implies* $m \leq n$ *since* n *is maximal in* $\mathbb{N}_\bot$.

   $MR_{\sigma\to\tau}$ *contains* $\bot_{\sigma\to\tau}$, *since for all* $N\ R_\sigma\ v$, $MN\ R_\tau\ \bot_{\sigma\to\tau}(v) = \bot_\tau$, *by induction hypothesis on* τ.

   If $f \in MR_{\sigma\to\tau}$ *and* $g \leq f$, *then for all* $N\ R_\sigma\ v$, $MN\ R_\tau\ f(v)$ *by definition hence* $MN\ R_\tau\ g(v)$ *since* MNR_τ *is downward closed by induction hypothesis on* τ. *So* $g \in MR_{\sigma\to\tau}$.

   If $(f_i)_{i\in I}$ *is a directed family in* MR_τ, *then for all* $N\ R_\sigma\ v$, $MN\ R_\tau\ f_i(v)$. *Since* MNR_τ *is closed under directed sups by induction hypothesis on* τ, $MN\ R_\tau \sup_{i\in I}(f_i(v)) = (\sup_{i\in I} f_i)(v)$. *So* $M\ R_{\sigma\to\tau} \sup_{i\in I} f_i$.

8. Show that if $M \precsim_\tau N$ and $M\ R_\tau\ u$, then $N\ R_\tau\ u$. In other words, the set $R_\tau u = \{M : \tau \mid M\ R_\tau\ u\}$ is *upward closed* in $\precsim_\tau$.

   By induction on types again. If $M \precsim_{\mathtt{Nat}} N$ *and* $M\ R_{\mathtt{Nat}}\ u$, *then either* $u = \bot$ *and* $N\ R_{\mathtt{Nat}}\ u$ *is by definition, or* $u = n \in \mathbb{N}$, $\underline{n} \precsim_{\mathtt{Nat}} M$. *Now,* $\precsim_{\mathtt{Nat}}$ *is transitive. Precisely, for every* E *of the right type, and every well-typed substitution* θ *of ground terms for variables, for every* $m \in \mathbb{N}$, *the latter states that if* $E \cdot \underline{n} \to^* \_ \cdot \underline{m}$ *then* $E \cdot \underline{M} \to^* \_ \cdot \underline{m}$, *and* $M \precsim_{\mathtt{Nat}} N$ *then implies that* $E \cdot \underline{N} \to^* \_ \cdot \underline{m}$. *So* $\underline{n} \precsim_{\mathtt{Nat}} N$. *Since* $u = n$, $N\ R_{\mathtt{Nat}}\ u$.

On function types $\sigma \to \tau$, the key argument is that whenever $M \precsim_{\sigma\to\tau} N$, then for every $P : \sigma$, $MP \precsim_\tau NP$, i.e., that for every E of the right type, and every well-typed substitution θ of ground terms for variables, for every $m \in \mathbb{N}$, if $E \cdot MP \to^* \_ \cdot \underline{m}$ then $E \cdot NP \to^* \_ \cdot \underline{m}$. The only reduction $E \cdot MP \to^* \_ \cdot \underline{m}$ must use $(DApp)$ as the first rule, hence be of the form $E \cdot MP \to E[\_P] \cdot M \to^* \_ \cdot \underline{m}$. Since $M \precsim_{\sigma\to\tau} N$ one must have $E[\_P] \cdot N \to^* \_ \cdot \underline{m}$, hence $E \cdot NP \to^* \_ \cdot \underline{m}$, using $(DApp)$.

So assume that $M \precsim_{\sigma\to\tau} N$ and $M\ R_{\sigma\to\tau}\ f$. For all $P\ R_\sigma\ v$, $MP\ R_\tau\ f(v)$. We have seen that $MP \precsim_\tau NP$, so by induction hypothesis on τ, $NP\ R_\tau\ f(v)$. So $N\ R_{\sigma\to\tau}\ f$.

9. Given a well-typed substitution θ, and an environment ρ, write $\theta\ R_*\ \rho$ iff $x_\sigma\theta\ R_\sigma\ \rho(x_\sigma)$ for every variable x_σ in the domain of θ.

   Prove the *Basic Lemma* : if $\theta\ R_*\ \rho$, and M is a term of type τ, then $M\theta\ R_\tau\ [\![M]\!]\,\rho$.

   By induction on the size of M this time.
   - *If M is a variable x_σ, then this is the induction hypothesis.*
   - *If M is an application NP, with $P : \sigma$, then by induction hypothesis $N\theta\ R_{\sigma\to\tau}\ [\![N]\!]\,\rho$ and $P\theta\ R_\sigma\ [\![P]\!]\,\rho$, so $M\theta = (N\theta)(P\theta)\ R_\tau\ [\![N]\!]\,\rho([\![P]\!]\,\rho) = [\![M]\!]\,\rho$ by definition of $R_{\sigma\to\tau}$.*
   - *If M is an abstraction $\lambda x_\sigma \cdot N$, and $\tau = \sigma \to \sigma'$, then we must show that for all $P\ R_\sigma\ v$ $((\lambda x_\sigma \cdot N)\theta)P\ R_{\sigma'}\ [\![N]\!]\,(\rho[x_\sigma := v])$.*
     Using α-renaming, we may assume x_σ fresh, and therefore $\theta \cup [x_\sigma := P]$ to be a meaningful well-typed substitution θ' such that $N\theta' = N\theta[x_\sigma := P]$. Note that for every variable y in the domain of θ', $y\theta'$ is in logical relation to $\rho'(y)$, where $\rho' = \rho[x_\sigma := v]$. This is by assumption if y is in the domain of θ, and follows from $P\ R_\sigma\ v$ if $y = x_\sigma$.
     So by induction hypothesis $N\theta'\ R_{\sigma'}\ [\![N]\!]\,\rho'$. We conclude since $N\theta' = N\theta[x_\sigma := P] \precsim_{\sigma'} ((\lambda x_\sigma \cdot N)\theta)P$ (Question 6, first item) and using Question 8.
   - *If M is a constant $\underline{n}$, $n \in \mathbb{N}$, then we must show that $\underline{n} \precsim_{\mathtt{Nat}} \underline{n}$. This is obvious.*
   - *If M is the constant* `pred`*, then we must show that for all $P\ R_{\mathtt{Nat}}\ v$,* `pred` $P\ R_{\mathtt{Nat}}$ $[\![\mathtt{pred}]\!]\,\rho(v)$.
     If $v = \bot$ or if $v = 0$, then $[\![\mathtt{pred}]\!]\,\rho(v) = \bot$, so this results from the fact that `pred` $PR_{\mathtt{Nat}}$ *contains $\bot$ (Question 7, last item).*
     Otherwise, $v = n + 1$ for some $n \in \mathbb{N}$, and we must show that `pred` $P\ R_{\mathtt{Nat}}\ n$ *under the assumption that $P\ R_{\mathtt{Nat}}\ n + 1$. Equivalently, we must show $\underline{n} \precsim_{\mathtt{Nat}}$* `pred` P *under the assumption $\underline{n+1} \precsim_{\mathtt{Nat}} P$. This is Question 6, item 4.*
   - *The case $M =$* `succ` *similarly follows from Question 6, item 3.*
   - *The case $M =$* `ifz` *similarly follows from Question 6, item 5 (if $v = 0$) or item 6 (if $v = n + 1$ for some $n \in \mathbb{N}$).*
   - *Finally, we deal with the case $M = Y_\tau$. We must show that for all $P\ R_{\tau\to\tau}\ f$, $YP\ R_\tau$ $\sup_{n\in\mathbb{N}} f^n(\bot)$. Since YPR_τ is Scott-closed (Question 7), it is enough to show that $YP\ R_\tau\ f^n(\bot)$ for every $n \in \mathbb{N}$. We show this by induction on $n \in \mathbb{N}$. If $n = 0$, this is obvious since YPR_τ contains $\bot$ (Question 7, last item). Otherwise, by induction hypothesis $YP\ R_\tau\ f^{n-1}(\bot)$. Since $P\ R_{\tau\to\tau}\ f$, by definition of $R_{\tau\to\tau}$, $P(YP)\ R_\tau$*

$f^n(\bot)$. But $P(YP) \precsim_\tau YP$ by Question 6, item 2. Since $R_\tau f^n(\bot)$ is upward-closed (Question 8), $YP\ R_\tau\ f^n(\bot)$, and we conclude.

10. Conclude that *computational adequacy* holds : given a ground configuration $E \cdot M$ such that $E[M] : \mathtt{Nat}$, $[\![E[M]]\!] = n \in \mathbb{N}$ if and only if $E \cdot M \to^* \_ \cdot \underline{n}$.

    One direction is Question 4. Conversely, if $[\![E[M]]\!] = n \in \mathbb{N}$, then $E[M]\ R_{\mathtt{Nat}}\ n$ by Question 9, using the identity substitution (since $E \cdot M$ is ground). By definition, $\underline{n} \precsim_{\mathtt{Nat}} E[M]$. Using an empty context, $\_ \cdot E[M] \to^* \_ \cdot \underline{n}$. Now the first machine rules in the latter reduction must be redex discovery rules, until we reach the configuration $E \cdot M$.

    Formally, we show that if $E' \cdot E[M] \to^* \_ \cdot \underline{n}$, then $E'[E] \cdot M \to^* \_ \cdot \underline{n}$, by induction on the size of E. If $E = \_$, this is clear. If $E = E_1 N$, then the only applicable rule is $(DApp)$, yielding $E' \cdot E[M] \to E'[\_N] \cdot E_1[M] \to^* \_ \cdot \underline{n}$. If $E = \mathtt{succ}\, E_1$, then the first two rules must be $(DApp)$ and $(DPred)$, yielding $E' \cdot E[M] \to E'[\_E_1[M]] \cdot \mathtt{succ} \to E'[\mathtt{succ}\, \_] \cdot E_1[M] \to^* \_ \cdot \underline{n}$; if $E = \mathtt{pred}\, E_1$, then these are $(DApp)$ and $(DSucc)$; if $E = \mathtt{ifz}\ E_1\ N\ P$, then these are $(DApp)$ (three times) and (DIf).