Expressions and Formulae

$$\begin{array}{lll} \textbf{Expressions} & e, e', \ldots & ::= a \mid 0 \mid \mathsf{s}(e) \mid e + e' \mid e \times e' \mid e \leq e' \\ \textbf{Formulae} & A, B, \ldots & ::= \mathsf{isnul}!(e) \mid A \Rightarrow B \mid \forall a^{\mathbb{N}} A \end{array}$$

Representation of integers as expressions: let $\overline{0} := 0$ and, for all integer n, let $\overline{n+1} := \mathsf{s}(\overline{n})$.
Let $\neg A := A \Rightarrow \mathsf{isnul}!(\overline{1})$.

Proof-terms

Syntax and reductions:

$$\begin{array}{lll} \textbf{Continuations} & E, \ldots & ::= \alpha \mid t :: E \\ \textbf{Terms} & t, u, \ldots & ::= x \mid \lambda x.t \mid \mu\alpha c \\ \textbf{Commands} & c, \ldots & ::= \langle t \bullet E \rangle \end{array} \qquad \begin{array}{lll} \langle \mu\alpha c \bullet E \rangle & \longrightarrow & \{{}^{E}\!/_{\alpha}\} c \\ \langle \lambda x.t \bullet u :: E \rangle & \longrightarrow & \langle \{{}^{u}\!/_{x}\} t \bullet E \rangle \end{array}$$

Let $\mathcal{E}$ denote the set of continuations, and $\mathcal{T}$ denote the set of terms.
Church's numerals as terms:

$$\begin{array}{lll} c_0 & := & \langle x \bullet \alpha \rangle \\ c_{n+1} & := & \langle f \bullet (\mu\alpha c_n) :: \alpha \rangle \\ \underline{n} & := & \lambda x.\lambda f.\mu\alpha c_n \end{array}$$

We admit that there are terms $\mathbf{s}$ and $\mathbf{rec}$ such that, for all t, u_0, u_1, E, and all integer n,

$$\begin{array}{lll} \langle \mathbf{s} \bullet \underline{n} :: t :: E \rangle & \longrightarrow^* & \langle t \bullet \underline{n+1} :: E \rangle \\ \langle \mathbf{rec} \bullet u_0 :: u_1 :: \underline{0} :: E \rangle & \longrightarrow^* & \langle u_0 \bullet E \rangle \\ \langle \mathbf{rec} \bullet u_0 :: u_1 :: \underline{n+1} :: E \rangle & \longrightarrow^* & \langle u_1 \bullet \underline{n} :: (\mu\alpha \langle \mathbf{rec} \bullet u_0 :: u_1 :: \underline{n} :: \alpha \rangle) :: E \rangle \end{array}$$

Realizability semantics

Let $\perp$ be an arbitrary set of commands, stable under anti-reduction (if $c \longrightarrow c'$ and $c' \in \perp$ then $c \in \perp$).
If $\mathcal{U}$ is a set of continuations, $\mathcal{U}^{\perp} := \{t \in \mathcal{T} \mid \forall E \in \mathcal{U}, \langle t \bullet E \rangle \in \perp\}$
If $\mathcal{U}$ is a set of terms, $\mathcal{U}^{\perp} := \{E \in \mathcal{E} \mid \forall t \in \mathcal{U}, \langle t \bullet E \rangle \in \perp\}$

The semantics below interprets expressions as integers and formulae as sets of continuations and sets of terms.
A valuation σ is a mapping from expression variables (a, etc) to integers.

$$\begin{array}{lll} [\![a]\!]_\sigma & := & \sigma(a) \\ [\![0]\!]_\sigma & := & 0 \\ [\![\mathsf{s}(e)]\!]_\sigma & := & [\![e]\!]_\sigma + 1 \\ [\![e_1 + e_2]\!]_\sigma & := & [\![e_1]\!]_\sigma + [\![e_2]\!]_\sigma \\ [\![e_1 \times e_2]\!]_\sigma & := & [\![e_1]\!]_\sigma \times [\![e_2]\!]_\sigma \\ [\![e_1 \leq e_2]\!]_\sigma & := & 1 \qquad \text{if } [\![e_1]\!]_\sigma \leq [\![e_2]\!]_\sigma \\ [\![e_1 \leq e_2]\!]_\sigma & := & 0 \qquad \text{if } [\![e_1]\!]_\sigma > [\![e_2]\!]_\sigma \end{array}$$

$$\begin{array}{lll} [\mathsf{isnul}!(e)]_\sigma & := & \mathcal{E} \qquad \text{if } [\![e]\!]_\sigma \neq 0 \\ [\mathsf{isnul}!(e)]_\sigma & := & \emptyset \qquad \text{if } [\![e]\!]_\sigma = 0 \\ [A \Rightarrow B]_\sigma & := & [\![A]\!]_\sigma :: [B]_\sigma \\ \left[\forall a^{\mathbb{N}} A\right]_\sigma & := & \bigcup_{n \in \mathbb{N}} \left(\{\underline{n}\} :: [A]_{\sigma, a \mapsto n} \right) \\ \hline [\![A]\!]_\sigma & := & [A]_\sigma{}^{\perp} \end{array}$$

where $\mathcal{U} :: \mathcal{V} := \{u :: E \mid u \in \mathcal{U}, E \in \mathcal{V}\}$

Exercise 1 : Properties of the system

1. Give a term **ifz** such that for all integers n and all u_0 and u_1 and E we have

$$\begin{array}{rl} \langle \mathbf{ifz} \bullet \underline{0} :: u_0 :: u_1 :: E\rangle & \longrightarrow^* \langle u_0 \bullet E\rangle \\ \langle \mathbf{ifz} \bullet \underline{n+1} :: u_0 :: u_1 :: E\rangle & \longrightarrow^* \langle u_1 \bullet E\rangle \end{array}$$

(you may use **rec**)

Correction : Let **ifz** $:= \lambda n x_0 x_1 . \mu\alpha \langle \mathbf{rec} \bullet x_0 :: (\lambda y_0 y_1 . x_1) :: n :: \alpha\rangle$

2. Show that for all integers n, $[\![\overline{n}]\!]_\sigma = n$ and that for all expressions e', $[\![\{\overline{n}/_a\}e']\!]_\sigma = [\![e']\!]_{\sigma,a\mapsto n}$.

Correction : The first point is by induction on n:
$[\![\overline{0}]\!]_\sigma = [\![\mathsf{0}]\!]_\sigma = 0$ and $[\![\overline{n+1}]\!]_\sigma = [\![\mathsf{s}(\overline{n})]\!]_\sigma = [\![\overline{n}]\!]_\sigma + 1 = n+1$.
The second point is proved by induction on e':

$$\begin{array}{ll} [\![\{\overline{n}/_a\}a]\!]_\sigma & = n = [\![a]\!]_{\sigma,a\mapsto n} \\ [\![\{\overline{n}/_a\}b]\!]_\sigma & = b = [\![b]\!]_{\sigma,a\mapsto n} \\ [\![\{\overline{n}/_a\}\mathsf{0}]\!]_\sigma & = 0 = [\![\mathsf{0}]\!]_{\sigma,a\mapsto n} \\ [\![\{\overline{n}/_a\}\mathsf{s}(e_1)]\!]_\sigma & = [\![\mathsf{s}(\{\overline{n}/_a\}e_1)]\!]_\sigma = [\![\{\overline{n}/_a\}e_1]\!]_\sigma + 1 = [\![e_1]\!]_{\sigma,a\mapsto n} + 1 = [\![\mathsf{s}(e_1)]\!]_{\sigma,a\mapsto n} \\ [\![\{\overline{n}/_a\}(e_1+e_2)]\!]_\sigma & = [\![\{\overline{n}/_a\}e_1 + \{\overline{n}/_a\}e_2]\!]_\sigma = [\![\{\overline{n}/_a\}e_1]\!]_\sigma + [\![\{\overline{n}/_a\}e_2]\!]_\sigma \\ & = [\![e_1]\!]_{\sigma,a\mapsto n} + [\![e_2]\!]_{\sigma,a\mapsto n} = [\![e_1+e_2]\!]_{\sigma,a\mapsto n} \\ [\![\{\overline{n}/_a\}(e_1\times e_2)]\!]_\sigma & = [\![\{\overline{n}/_a\}e_1 \times \{\overline{n}/_a\}e_2]\!]_\sigma = [\![\{\overline{n}/_a\}e_1]\!]_\sigma \times [\![\{\overline{n}/_a\}e_2]\!]_\sigma \\ & = [\![e_1]\!]_{\sigma,a\mapsto n} \times [\![e_2]\!]_{\sigma,a\mapsto n} = [\![e_1+e_2]\!]_{\sigma,a\mapsto n} \\ [\![\{\overline{n}/_a\}(e_1\le e_2)]\!]_\sigma & = [\![\{\overline{n}/_a\}e_1 \le \{\overline{n}/_a\}e_2]\!]_\sigma \\ & = 1 = [\![e_1\le e_2]\!]_{\sigma,a\mapsto n} \text{ if } [\![\{\overline{n}/_a\}e_1]\!]_\sigma \le [\![\{\overline{n}/_a\}e_2]\!]_\sigma \text{ (i.e. } [\![e_1]\!]_{\sigma,a\mapsto n} \le [\![e_2]\!]_{\sigma,a\mapsto n}) \\ & = 0 = [\![e_1\le e_2]\!]_{\sigma,a\mapsto n} \text{ if } [\![\{\overline{n}/_a\}e_1]\!]_\sigma > [\![\{\overline{n}/_a\}e_2]\!]_\sigma \text{ (i.e. } [\![e_1]\!]_{\sigma,a\mapsto n} > [\![e_2]\!]_{\sigma,a\mapsto n}) \end{array}$$

3. Show that for all formulae A, we have $\left[\{\overline{n}/_a\}A\right]_\sigma = [A]_{\sigma,a\mapsto n}$ and $[\![\{\overline{n}/_a\}A]\!]_\sigma = [\![A]\!]_{\sigma,a\mapsto n}$.

Correction : We first need that $(\{\overline{n}/_a\}A)^\perp = \{\overline{n}/_a\}A^\perp$ (easy induction on A).
Then we prove that $\left[\{\overline{n}/_a\}A\right]_\sigma = [A]_{\sigma,a\mapsto n}$ by induction on A (positive formulae first, then negative formulae):

$$\begin{array}{ll} \left[\{\overline{n}/_a\}\mathsf{notnull}(e)\right]_\sigma & = \mathcal{E} = [\mathsf{notnull}(e)]_{\sigma,a\mapsto n} \quad \text{if } [\![e]\!]_{\sigma,a\mapsto n} = [\![\{\overline{n}/_a\}e]\!]_\sigma \neq 0 \\ \left[\{\overline{n}/_a\}\mathsf{notnull}(e)\right]_\sigma & = \emptyset = [\mathsf{notnull}(e)]_{\sigma,a\mapsto n} \quad \text{if } [\![e]\!]_{\sigma,a\mapsto n} = [\![\{\overline{n}/_a\}e]\!]_\sigma = 0 \\ \left[\{\overline{n}/_a\}(A\wedge B)\right]_\sigma & = \left[\{\overline{n}/_a\}A \wedge \{\overline{n}/_a\}B\right]_\sigma :: \left[\{\overline{n}/_a\}A\right]_\sigma :: \left[\{\overline{n}/_a\}B\right]_\sigma = [A]_{\sigma,a\mapsto n} :: [B]_{\sigma,a\mapsto n} = [A\wedge B]_{\sigma,a\mapsto n} \\ \left[\{\overline{n}/_a\}(e\wedge B)\right]_\sigma & = \left[\{\overline{n}/_a\}e \wedge \{\overline{n}/_a\}B\right]_\sigma = \{\overline{[\![\{\overline{n}/_a\}e]\!]_\sigma}\} :: \left[\{\overline{n}/_a\}B\right]_\sigma = \{\overline{[\![e]\!]_{\sigma,a\mapsto n}}\} :: \left[\{\overline{n}/_a\}B\right]_\sigma = [e\wedge B]_{\sigma,a\mapsto n} \\ \left[\{\overline{n}/_a\}\exists b.A\right]_\sigma & = \left[\exists b.\{\overline{n}/_a\}A\right]_\sigma = \bigcup_{m\in\mathbb{N}} \left[\{\overline{n}/_a\}A\right]_{\sigma,b\mapsto m} = \bigcup_{m\in\mathbb{N}} [A]_{\sigma,b\mapsto m,a\mapsto n} = [\exists b.A]_{\sigma,a\mapsto n} \\ \left[\{\overline{n}/_a\}N\right]_\sigma & = \left[(\{\overline{n}/_a\}N)^\perp\right]_\sigma{}^\perp = \left[\{\overline{n}/_a\}N^\perp\right]_\sigma{}^\perp = \left[N^\perp\right]_{\sigma,a\mapsto n}{}^\perp = [N]_{\sigma,a\mapsto n} \end{array}$$

Finally we get $[\![\{\overline{n}/_a\}A]\!]_\sigma = \left[\{\overline{n}/_a\}A\right]_\sigma{}^{\perp\perp} = [A]_{\sigma,a\mapsto n}{}^{\perp\perp} = [\![A]\!]_{\sigma,a\mapsto n}$

For the second point:
$$[\![P^\perp]\!]_\sigma = \left[P^\perp\right]_\sigma{}^{\perp\perp} = \left[P^{\perp\perp}\right]_\sigma{}^{\perp\perp\perp} = [P]_\sigma{}^{\perp\perp\perp} = [\![P]\!]_\sigma{}^\perp$$
$$[\![N^\perp]\!]_\sigma = \left[N^\perp\right]_\sigma{}^{\perp\perp} = [N]_\sigma{}^\perp = [N]_\sigma{}^{\perp\perp\perp} = [\![N]\!]_\sigma{}^\perp$$

Exercise 2 : Realizability in arithmetics

In this exercise, we show how to extract a witness from a classical proof of a Σ^0_1-formula, i.e. a closed formula of the form $\exists a A(a)$ where $A(a)$ is a quantifier-free formula of arithmetics.
We work in a particular setting where such a formula is expressed in the shape of $\neg\forall a^{\mathbb{N}}\neg\mathsf{isnull}(e(a))$ (c.f. our syntax for formulae on the other page). We admit that this shape brings no loss of generality. Moreover, such an expression $e(a)$, with one free variable a, expresses a primitive recursive function from $\mathbb{N}$ to $\mathbb{N}$.
In this exercise you will not need the typing system for proof-terms, but only what is provided by the Adequacy Lemma:
a proof t_0 of a formula $\neg\forall a^{\mathbb{N}}\neg\mathsf{isnull}(e(a))$ is such that, for all possible $\perp$, $t_0 \in [\![\neg\forall a^{\mathbb{N}}\neg\mathsf{isnull}(e(a))]\!]$.
We thus start with such a positive term t_0.

1. Show that if $t \in [\![\mathsf{isnull}(\overline{n})]\!]_\sigma$ with $n\neq 0$, then for all continuations E we have $\langle t\bullet E\rangle \in \perp$.

Correction : If $n\neq 0$ then $[\![\overline{n}]\!]_\sigma \neq 0$, so $[\mathsf{isnull}(\overline{n})]_\sigma = \mathcal{E}$, and by definition of $[\![\mathsf{isnull}(\overline{n})]\!]_\sigma$, $t \in [\![\mathsf{isnull}(\overline{n})]\!]_\sigma$ means that for all continuations E we have $\langle t\bullet E\rangle \in \perp$.

2. Let f be the primitive recursive function defined by: for any integer n, $f(n) := [\![e(a)]\!]_{a\mapsto n}$.
   Let $\underline{f}$ be an term representing f in the sense that,
   for any integer n, and term t and any continuation E, $\langle \underline{f} \bullet \underline{n} :: t :: E\rangle \longrightarrow^* \langle t \bullet \underline{f(n)} :: E\rangle$
   Let $d_f := \lambda nxy.\mu\alpha.\langle \underline{f} \bullet n :: (\lambda p.\mu\alpha_1.\langle \mathbf{ifz} \bullet p :: x :: y :: \alpha_1\rangle) :: \alpha\rangle$
   Show that for any integer n, any u_0 and u_1 and E, we have
   $\langle d_f \bullet \underline{n} :: u_0 :: u_1 :: E\rangle \longrightarrow^* \langle u_0 \bullet E\rangle$ if $f(n) = 0$
   $\langle d_f \bullet \underline{n} :: u_0 :: u_1 :: E\rangle \longrightarrow^* \langle u_1 \bullet E\rangle$ if $f(n) \neq 0$
   Correction :

$$\begin{array}{lll}
\langle d_f \bullet \underline{n} :: u_0 :: u_1 :: E\rangle & \longrightarrow^* & \langle \mu\alpha.\langle \underline{f} \bullet \underline{n} :: (\lambda p.\mu\alpha_1.\langle \mathbf{ifz} \bullet p :: u_0 :: u_1 :: \alpha_1\rangle) :: \alpha\rangle \bullet E\rangle \\
& \longrightarrow^* & \langle \underline{f} \bullet \underline{n} :: (\lambda p.\mu\alpha_1.\langle \mathbf{ifz} \bullet p :: u_0 :: u_1 :: \alpha_1\rangle) :: E\rangle \\
& \longrightarrow^* & \langle \lambda p.\mu\alpha_1.\langle \mathbf{ifz} \bullet p :: u_0 :: u_1 :: \alpha_1\rangle \bullet \underline{f(n)} :: E\rangle \\
& \longrightarrow^* & \langle \mu\alpha_1.\langle \mathbf{ifz} \bullet \underline{f(n)} :: u_0 :: u_1 :: \alpha_1\rangle \bullet E\rangle \\
& \longrightarrow^* & \langle \mathbf{ifz} \bullet \underline{f(n)} :: u_0 :: u_1 :: E\rangle
\end{array}$$

   If $f(n) = 0$, this reduces to $\langle u_0 \bullet E\rangle$.
   Otherwise, this reduces to $\langle u_1 \bullet E\rangle$.

3. Let **stop** be an arbitrary term and **go** be an arbitrary continuation.
   We now take a particular orthogonality set defined by

$$\bot := \{c \mid \text{ there exists } n \text{ such that } f(n) = 0 \text{ and } c \longrightarrow^* \langle \mathbf{stop} \bullet \underline{n} :: \mathbf{go}\rangle\}$$

   Let $t_1 := \lambda nx.\mu\alpha.\langle d_f \bullet n :: (\mu\alpha_0.\langle \mathbf{stop} \bullet n :: \mathbf{go}\rangle) :: x :: \alpha\rangle$.
   Show that, for all integer n and all $E \in [\neg\mathsf{isnull}(e(\overline{n}))]$, we have $t_1 \perp \underline{n} :: E$
   (distinguish the cases where $f(n) = 0$ and $f(n) \neq 0$).
   Correction : Let E be in

$$\begin{array}{rl}
[\neg\mathsf{isnull}(e(\overline{n}))] = & [\![\mathsf{isnull}(e(\overline{n}))]\!] :: \left[\mathsf{isnull}(\overline{1})\right] \\
= & [\![\mathsf{isnull}(e(\overline{n}))]\!] :: \mathcal{E}
\end{array}$$

   E is of the form $u :: E'$ with $u \in [\![\mathsf{isnull}(e(\overline{n}))]\!]$.
   Now $\langle t_1 \bullet \underline{n} :: E\rangle = \langle t_1 \bullet \underline{n} :: u :: E'\rangle \longrightarrow^* \langle d_f \bullet \underline{n} :: (\mu\alpha_0.\langle \mathbf{stop} \bullet \underline{n} :: \mathbf{go}\rangle) :: u :: E'\rangle$.
   If $f(n) = 0$ then this reduces to $\langle (\mu\alpha_0.\langle \mathbf{stop} \bullet \underline{n} :: \mathbf{go}\rangle) \bullet E'\rangle \longrightarrow^* \langle \mathbf{stop} \bullet \underline{n} :: \mathbf{go}\rangle$, which is in $\bot$ (and so is $\langle t_1 \bullet E\rangle$).
   If $f(n) \neq 0$ this reduces to $\langle u \bullet E'\rangle$, but we know by definition of f that $[\![e(a)]\!]_{a\mapsto n} \neq 0$, i.e. $[\![e(\overline{n})]\!] \neq 0$, so $[\mathsf{isnull}(e(\overline{n}))] = \mathcal{E}$. Hence, $u \in [\![\mathsf{isnull}(e(\overline{n}))]\!]$ entails $\langle u \bullet E'\rangle \in \bot$ (so again $\langle t_1 \bullet E\rangle \in \bot$).

4. Show that $t_1 \in [\![\forall a^{\mathbb{N}} \neg\mathsf{isnull}(e(a)))]\!]$
   Correction : Notice that $\left[\forall a^{\mathbb{N}} \neg\mathsf{isnull}(e(a)))\right]$ is $\bigcup_{n\in\mathbb{N}} \left(\{\underline{n}\} :: [\neg\mathsf{isnull}(e(a))]_{a\mapsto n}\right)$.
   So in order to show $t_1 \in [\![\forall a^{\mathbb{N}} \neg\mathsf{isnull}(e(a)))]\!]$ we must show that for all n and all $E \in [\neg\mathsf{isnull}(e(a))]_{a\mapsto n} = [\neg\mathsf{isnull}(e(\overline{n}))]$ we have $t_1 \perp \underline{n} :: E$. This is exactly the previous question.

5. Show that $t_1 :: \mathbf{go} \in \left[\neg\forall a^{\mathbb{N}} \neg\mathsf{isnull}(e(a))\right]$
   Correction : $\left[\neg\forall a^{\mathbb{N}} \neg\mathsf{isnull}(e(a))\right]$ is $[\![\forall a^{\mathbb{N}} \neg\mathsf{isnull}(e(a))]\!] :: \left[\mathsf{isnull}(\overline{1})\right]$, which is $[\![\forall a^{\mathbb{N}} \neg\mathsf{isnull}(e(a))]\!] :: \mathcal{E}$, so it suffices to notice that $t_1 \in [\![\forall a^{\mathbb{N}} \neg\mathsf{isnull}(e(a)))]\!]$ from the previous question, and $\mathbf{go} \in \mathcal{E}$.

6. Show that $\langle t_0 \bullet t_1 :: \mathbf{go}\rangle \longrightarrow^* \langle \mathbf{stop} \bullet \underline{n} :: \mathbf{go}\rangle$ for some integer n such that $f(n) = 0$.
   Correction : We have $t_0 \in [\![\neg\forall a^{\mathbb{N}} \neg\mathsf{isnull}(e(a))]\!]$ and $t_1 :: \mathbf{go} \in \left[\neg\forall a^{\mathbb{N}} \neg\mathsf{isnull}(e(a))\right]$, so $\langle t_0 \bullet t_1 :: \mathbf{go}\rangle \in \bot$, which precisely means that $\langle t_0 \bullet t_1 :: \mathbf{go}\rangle \longrightarrow^* \langle \mathbf{stop} \bullet \underline{n} :: \mathbf{go}\rangle$ for some integer n such that $f(n) = 0$.