Syntax: indices and terms

%datatype *index*
%name *index* n α

$$
\begin{array}{lcl}
n & ::= & 0 \\
  & \mid & n+1
\end{array}
$$

%datatype *term*
%name *term* t

$$
\begin{array}{lcl}
t & ::= & n \\
  & \mid & t_1\, t_2 \\
  & \mid & \lambda t \\
  & \mid & \mathbf{catch}\, t \\
  & \mid & \mathbf{throw}\, \alpha\, t
\end{array}
$$

$$
\begin{array}{lcl}
t & ::= & n \\
  & \mid & t_1\, t_2 \\
  & \mid & \lambda t \\
  & \mid & \mathbf{get\text{-}context}\, t \\
  & \mid & \mathbf{set\text{-}context}\, \alpha\, t
\end{array}
$$

Definition of Safety: vectors and tables

%datatype *vector*
%name *vector* $\mathcal{I}$

$$\begin{array}{lcl} \mathcal{I} & ::= & [\,] \\ & | & n :: \mathcal{I} \end{array}$$

%datatype *table*
%name *table* $\mathcal{I}_\mu$

$$\begin{array}{lcl} \mathcal{I}_\mu & ::= & [\,] \\ & | & \mathcal{I} :: \mathcal{I}_\mu \end{array}$$

Member and fetch

%judgment $n \in \mathcal{I}$
%judgment $\mathcal{I}(n_1) = n_2$
%judgment $\mathcal{I}_\mu(n) = \mathcal{I}$

Example of definition (fetch)

%judgment $\mathcal{I}(n_1) = n_2$

$$(n :: \mathcal{I})(0) = n \;^{[\text{fetch}_1^{\mathcal{I}}]}$$

$$(n :: \mathcal{I})(n_1 + 1) = n_2 \;^{[\text{fetch}_2^{\mathcal{I}}]} \quad \textit{when} \quad \mathcal{I}(n_1) = n_2$$

%mode $+\mathcal{I}(+n_1) = -n_2$
%worlds $()$ $\mathcal{I}(n_1) = n_2$
%terminates n_1 $\mathcal{I}(n_1) = n_2$
%unique $+\mathcal{I}(+n_1) = -1n_2$

Example of properties

%lemma $k \in \mathcal{I} \quad \Rightarrow \quad \mathcal{I}(n) = k \quad \textit{for some } n \;^{[\text{domain}]}$
%lemma $\mathcal{I}(n) = k \quad \Rightarrow \quad k \in \mathcal{I} \;^{[\text{target}]}$

Example of proof

%lemma $\quad k \in \mathcal{I} \quad \Rightarrow \quad \mathcal{I}(n) = k \quad \textit{for some } n \quad {}^{[\text{domain}]}$

Proof.

$$\dfrac{}{n \in (n :: \mathcal{I})^{\,[\text{member}_1]} \quad \Rightarrow \quad (n :: \mathcal{I})(0) = n^{\,[\text{fetch}_1^{\mathcal{I}}]} \quad [\text{domain}]}\,[\&1]$$

$$\dfrac{\begin{matrix}\mathcal{D}_1 \\ k \in \mathcal{I}\end{matrix} \quad \Rightarrow \quad \begin{matrix}\mathcal{D}_2 \\ \mathcal{I}(n) = k\end{matrix} \quad [\text{domain}]}{\dfrac{\begin{matrix}\mathcal{D}_1 \\ k \in \mathcal{I}\end{matrix}}{k \in (k' :: \mathcal{I})}\,[\text{member}_2] \quad \Rightarrow \quad \dfrac{\begin{matrix}\mathcal{D}_2 \\ \mathcal{I}(n) = k\end{matrix}}{(k' :: \mathcal{I})(n+1) = k}\,[\text{fetch}_2^{\mathcal{I}}] \quad [\text{domain}]}\,[\&2]$$

%mode $\quad +\mathcal{D}_1 \quad \Rightarrow \quad -\mathcal{D}_2 \quad {}^{[\text{domain}]}$
%worlds $\quad () \quad \mathcal{D}_1 \quad \Rightarrow \quad \mathcal{D}_2 \quad {}^{[\text{domain}]}$
%total $\quad (\mathcal{D}_1) \quad \mathcal{D}_1 \quad \Rightarrow \quad \mathcal{D}_2 \quad {}^{[\text{domain}]}$

%lemma $\quad \mathcal{I}(n) = k \quad \Rightarrow \quad k \in \mathcal{I} \quad {}^{[\text{target}]}$ (same realizer with different modes)

Definition of Safety

%judgment $\mathit{Safe}_{n}^{\mathcal{I},\mathcal{I}_\mu}(t)$

$$
\begin{array}{llll}
\mathit{Safe}_{n}^{\mathcal{I},\mathcal{I}_\mu}(g) & [\mathrm{safe}_1] & \mathit{when} & n \dot{-} g = k, \quad k \in \mathcal{I} \\
\mathit{Safe}_{n}^{\mathcal{I},\mathcal{I}_\mu}(t\,u) & [\mathrm{safe}_2] & \mathit{when} & \mathit{Safe}_{n}^{\mathcal{I},\mathcal{I}_\mu}(t), \quad \mathit{Safe}_{n}^{\mathcal{I},\mathcal{I}_\mu}(u) \\
\mathit{Safe}_{n}^{\mathcal{I},\mathcal{I}_\mu}(\lambda t) & [\mathrm{safe}_3] & \mathit{when} & \mathit{Safe}_{n+1}^{(n+1\,::\,\mathcal{I}),\mathcal{I}_\mu}(t) \\
\mathit{Safe}_{n}^{\mathcal{I},\mathcal{I}_\mu}(\mathbf{catch}\,t) & [\mathrm{safe}_4] & \mathit{when} & \mathit{Safe}_{n}^{\mathcal{I},(\mathcal{I}\,::\,\mathcal{I}_\mu)}(t) \\
\mathit{Safe}_{n}^{\mathcal{I},\mathcal{I}_\mu}(\mathbf{throw}\,\alpha\,t) & [\mathrm{safe}_5] & \mathit{when} & \mathcal{I}_\mu(\alpha) = \mathcal{I}', \quad \mathit{Safe}_{n}^{\mathcal{I}',\mathcal{I}_\mu}(t)
\end{array}
$$

Translation from local indices to global indices

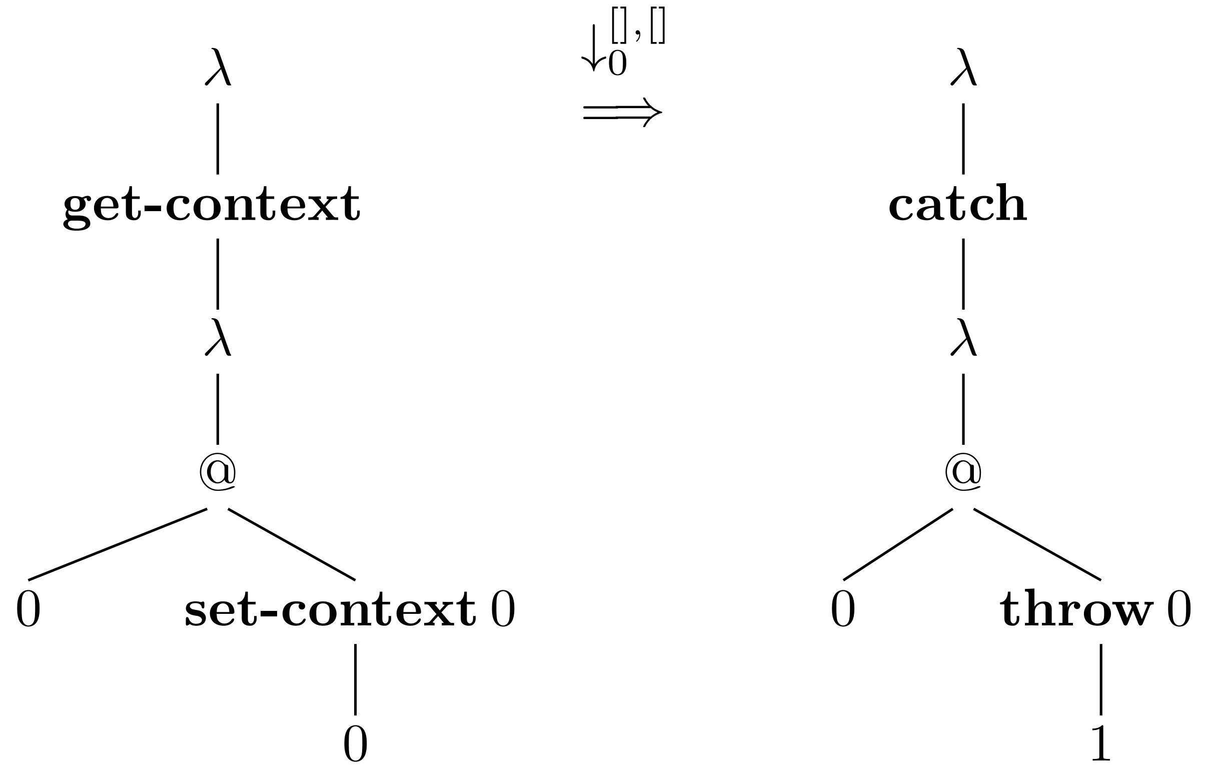
%judgment $\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(t_1) = t_2$

$\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(l) = g$	[$\downarrow_1$]	*when*	$n \mathbin{\dot{-}} \mathcal{I}(l) = g$
$\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(t\,u) = t'\,u'$	[$\downarrow_2$]	*when*	$\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(t) = t', \quad \downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(u) = u'$
$\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(\lambda t) = \lambda t'$	[$\downarrow_3$]	*when*	$\downarrow_{n+1}^{(n+1\,::\,\mathcal{I}),\mathcal{I}_\mu}(t) = t'$
$\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(\textbf{get-context}\,t) = \textbf{catch}\,t'$	[$\downarrow_4$]	*when*	$\downarrow_n^{\mathcal{I},(\mathcal{I}\,::\,\mathcal{I}_\mu)}(t) = t'$
$\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(\textbf{set-context}\,\alpha\,t) = \textbf{throw}\,\alpha\,t'$	[$\downarrow_5$]	*when*	$\mathcal{I}_\mu(\alpha) = \mathcal{I}', \quad \downarrow_n^{\mathcal{I}',\mathcal{I}_\mu}(t) = t'$

%lemma $\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(t) = t' \quad \Rightarrow \quad \mathit{Safe}_n^{\mathcal{I},\mathcal{I}_\mu}(t')$ [$\downarrow$·safe]

%lemma $\mathit{Safe}_n^{\mathcal{I},\mathcal{I}_\mu}(t') \quad \Rightarrow \quad \downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(t) = t'$ *for some* t [safe·image]

Example



%solve $\_$:
$$\downarrow_0^{[\,],[\,]}(\lambda\mathbf{get\text{-}context}\;\lambda(0\,(\mathbf{set\text{-}context}\;0\;0))) = \lambda\mathbf{catch}\;\lambda(0\,(\mathbf{throw}\;0\;1))$$

%solve $\_$: $d_1 \colon \mathit{Safe}_0^{[\,],[\,]}(\lambda\mathbf{catch}\;\lambda(0\,(\mathbf{throw}\;0\;1)))$
$$\Rightarrow \quad \sqcup \colon \downarrow_0^{[\,],[\,]}(t) = \lambda\mathbf{catch}\;\lambda(0\,(\mathbf{throw}\;0\;1)) \qquad [\text{safe}\cdot\text{image}]$$