1 Safety, local indices and translation

1.1 Syntax

1.1.1 Index, indices and tables

%datatype *index*
%name *index* n α

$$n ::= 0 \mid n+1$$

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

$$\mathcal{I} ::= [\,] \mid n :: \mathcal{I}$$

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

$$\mathcal{I}_\mu ::= [\,] \mid \mathcal{I} :: \mathcal{I}_\mu$$

1.1.2 Term

%datatype *term*
%name *term* t

$$t ::= n \mid t_1\, t_2 \mid \lambda t \mid \mathbf{catch}\, t \mid \mathbf{throw}\, \alpha\, t$$

Remark. Syntax of safe λ_{ct}-terms:

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

1.2 Subtraction

%judgment $n_1 \dot{-} n_2 = n_3$

$n_1 \dot{-} 0 = n_1$ [minus$_1$]

$(n_1+1) \dot{-} (n_2+1) = n_3$ [minus$_2$] *when* $n_1 \dot{-} n_2 = n_3$

%mode $+n_1 \dot{-} +n_2 = -n_3$
%worlds $()$ $n_1 \dot{-} n_2 = n_3$
%terminates (n_1) $n_1 \dot{-} n_2 = n_3$
%unique $+n_1 \dot{-} +n_2 = -1n_3$

%lemma $\forall n{:}\, index \cdot n \dot{-} n = 0$ [minus-id]

Proof.

$$\frac{}{0{:}\, index \cdot \; 0 \dot{-} 0 = 0^{\,[\text{minus}_1]} \quad {}^{[\text{minus-id}]}}\,[\&1]$$

$$\frac{n{:}\, index \cdot \begin{array}{c}\mathcal{D}\\ n \dot{-} n = 0\end{array} \; {}^{[\text{minus-id}]}}{n+1{:}\, index \cdot \dfrac{\begin{array}{c}\mathcal{D}\\ n \dot{-} n = 0\end{array}}{(n+1) \dot{-} (n+1) = 0}\,[\text{minus}_2] \quad {}^{[\text{minus-id}]}}\,[\&2]$$

%mode $+n \cdot -\mathcal{D}$ [minus-id]
%worlds $()$ $n \cdot \mathcal{D}$ [minus-id]
%total (n) $n \cdot \mathcal{D}$ [minus-id]

$\square$

%lemma $n_1 \dot{-} (n_2+1) = n_3 \;\Rightarrow\; n_1 \dot{-} n_2 = (n_3+1)$ [minus-succ]

Proof.

$$\frac{}{\begin{array}{c}\mathcal{D}\\ (n_1+1) \dot{-} (0+1) = n_1\end{array} \;\Rightarrow\; (n_1+1) \dot{-} 0 = (n_1+1)^{\,[\text{minus}_1]} \quad {}^{[\text{minus-succ}]}}\,[\&1]$$

$$\frac{\begin{array}{c}\mathcal{D}_1\\ n_1 \dot{-} (n_2+1) = n_3\end{array} \;\Rightarrow\; \begin{array}{c}\mathcal{D}_2\\ n_1 \dot{-} n_2 = (n_3+1)\end{array} \; {}^{[\text{minus-succ}]}}{\dfrac{\begin{array}{c}\mathcal{D}_1\\ n_1 \dot{-} (n_2+1) = n_3\end{array}}{(n_1+1) \dot{-} ((n_2+1)+1) = n_3}\,[\text{minus}_2] \;\Rightarrow\; \dfrac{\begin{array}{c}\mathcal{D}_2\\ n_1 \dot{-} n_2 = (n_3+1)\end{array}}{(n_1+1) \dot{-} (n_2+1) = (n_3+1)}\,[\text{minus}_2] \quad {}^{[\text{minus-succ}]}}\,[\&2]$$

%mode $+\mathcal{D}_1 \;\Rightarrow\; -\mathcal{D}_2$ [minus-succ]
%worlds $()$ $\mathcal{D}_1 \;\Rightarrow\; \mathcal{D}_2$ [minus-succ]
%total $\mathcal{D}_1$ $\mathcal{D}_1 \;\Rightarrow\; \mathcal{D}_2$ [minus-succ]

$\square$

%lemma $n_1 \dot{-} n_2 = n_3 \;\Rightarrow\; n_1 \dot{-} n_3 = n_2$ [minus-swap]

Proof.

$$\frac{n_1{:}\, index \cdot \begin{array}{c}\mathcal{D}\\ n_1 \dot{-} n_1 = 0\end{array} \; {}^{[\text{minus-id}]}}{n_1 \dot{-} 0 = n_1^{\,[\text{minus}_1]} \;\Rightarrow\; \begin{array}{c}\mathcal{D}\\ n_1 \dot{-} n_1 = 0\end{array} \quad {}^{[\text{minus-swap}]}}\,[\&1]$$

$$\frac{\begin{array}{c}\begin{array}{c}\mathcal{D}_1\\ n_1 \dot{-} n_2 = n_3\end{array} \;\Rightarrow\; \begin{array}{c}\mathcal{D}_2\\ n_1 \dot{-} n_3 = n_2\end{array} \; {}^{[\text{minus-swap}]}\\ \dfrac{\begin{array}{c}\mathcal{D}_2\\ n_1 \dot{-} n_3 = n_2\end{array}}{(n_1+1) \dot{-} (n_3+1) = n_2}\,[\text{minus}_2] \;\Rightarrow\; \begin{array}{c}\mathcal{D}_3\\ (n_1+1) \dot{-} n_3 = (n_2+1)\end{array} \; {}^{[\text{minus-succ}]}\end{array}}{\dfrac{\begin{array}{c}\mathcal{D}_1\\ n_1 \dot{-} n_2 = n_3\end{array}}{(n_1+1) \dot{-} (n_2+1) = n_3}\,[\text{minus}_2] \;\Rightarrow\; \begin{array}{c}\mathcal{D}_3\\ (n_1+1) \dot{-} n_3 = (n_2+1)\end{array} \quad {}^{[\text{minus-swap}]}}\,[\&2]$$

%mode $+\mathcal{D}_1 \;\Rightarrow\; -\mathcal{D}_2$ [minus-swap]
%worlds $()$ $\mathcal{D}_1 \;\Rightarrow\; \mathcal{D}_2$ [minus-swap]
%total $\mathcal{D}_1$ $\mathcal{D}_1 \;\Rightarrow\; \mathcal{D}_2$ [minus-swap]

$\square$

1.2.1 Fetch (indices)

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

$(n :: \mathcal{I})(0) = n$ [fetch$_1^{\mathcal{I}}$]
$(n :: \mathcal{I})(n_1+1) = n_2$ [fetch$_2^{\mathcal{I}}$] *when* $\mathcal{I}(n_1) = n_2$

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

1.2.2 Fetch (table)

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

$(\mathcal{I} :: \mathcal{I}_\mu)(0) = \mathcal{I}$ $\left[\text{fetch}_1^{\mathcal{I}_\mu}\right]$

$(\mathcal{I}' :: \mathcal{I}_\mu)(\alpha+1) = \mathcal{I}$ $\left[\text{fetch}_2^{\mathcal{I}_\mu}\right]$ *when* $\mathcal{I}_\mu(\alpha) = \mathcal{I}$

%mode $+\mathcal{I}_\mu(+\alpha) = -\mathcal{I}$
%worlds $()$ $\mathcal{I}_\mu(\alpha) = \mathcal{I}$
%terminates α $\mathcal{I}_\mu(\alpha) = \mathcal{I}$
%unique $+\mathcal{I}_\mu(+\alpha) = -1\mathcal{I}$

1.2.3 Compute

%judgment $n_1 \dot{-} \mathcal{I}(n_2) = n_3$

$n \dot{-} \mathcal{I}(l) = g$ [compute$_1$] *when* $\mathcal{I}(l) = k,\quad n \dot{-} k = g$

%mode $+n_1 \dot{-} +\mathcal{I}(+n_2) = -n_3$
%worlds $()$ $n_1 \dot{-} \mathcal{I}(n_2) = n_3$
%terminates $\{\}$ $n_1 \dot{-} \mathcal{I}(n_2) = n_3$
%unique $+n_1 \dot{-} +\mathcal{I}(+n_2) = -1n_3$

2 Safe $\boldsymbol{\lambda}_{ct}$-terms

2.1 Safety

%judgment $n \in \mathcal{I}$

$n \in (n :: \mathcal{I})$ [member$_1$]
$n \in (n' :: \mathcal{I})$ [member$_2$] *when* $n \in \mathcal{I}$

%mode $+n \in +\mathcal{I}$
%worlds $()$ $n \in \mathcal{I}$
%terminates $\mathcal{I}$ $n \in \mathcal{I}$

%lemma $k \in \mathcal{I} \;\Rightarrow\; \mathcal{I}(n) = k$ *for some* n [domain]

Proof.

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

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

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

$\square$

%judgment $Safe_n^{\mathcal{I},\mathcal{I}_\mu}(t)$

$Safe_n^{\mathcal{I},\mathcal{I}_\mu}(g)$	[safe$_1$]	*when*	$n \dot{-} g = k,\quad k \in \mathcal{I}$
$Safe_n^{\mathcal{I},\mathcal{I}_\mu}(t\,u)$	[safe$_2$]	*when*	$Safe_n^{\mathcal{I},\mathcal{I}_\mu}(t),\quad Safe_n^{\mathcal{I},\mathcal{I}_\mu}(u)$
$Safe_n^{\mathcal{I},\mathcal{I}_\mu}(\lambda t)$	[safe$_3$]	*when*	$Safe_{n+1}^{(n+1 :: \mathcal{I}),\mathcal{I}_\mu}(t)$
$Safe_n^{\mathcal{I},\mathcal{I}_\mu}(\mathbf{catch}\, t)$	[safe$_4$]	*when*	$Safe_n^{\mathcal{I},(\mathcal{I} :: \mathcal{I}_\mu)}(t)$
$Safe_n^{\mathcal{I},\mathcal{I}_\mu}(\mathbf{throw}\, \alpha\, t)$	[safe$_5$]	*when*	$\mathcal{I}_\mu(\alpha) = \mathcal{I}',\quad Safe_n^{\mathcal{I}',\mathcal{I}_\mu}(t)$

%mode $Safe_{+n}^{+\mathcal{I},+\mathcal{I}_\mu}(+t)$
%worlds $()$ $Safe_n^{\mathcal{I},\mathcal{I}_\mu}(t)$
%terminates t $Safe_n^{\mathcal{I},\mathcal{I}_\mu}(t)$

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

%mode $\downarrow_{+n}^{+\mathcal{I},+\mathcal{I}_\mu}(+t) = -t'$
%worlds $()$ $\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(t) = t'$
%terminates t $\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(t) = t'$

%unique $\downarrow_{+n}^{+\mathcal{I},+\mathcal{I}_\mu}(+t) = -1t'$

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

Proof.

$$\frac{\begin{array}{c} \overset{\mathcal{D}_2}{k \in \mathcal{I}} \quad \Rightarrow \quad \overset{\mathcal{D}_{111}}{\mathcal{I}(l) = k} \quad [\text{domain}] \\ \overset{\mathcal{D}_3}{n \dot{-} g = k} \quad \Rightarrow \quad \overset{\mathcal{D}_{112}}{n \dot{-} k = g} \quad [\text{minus·swap}] \end{array}}{\dfrac{\overset{\mathcal{D}_3}{n \dot{-} g = k} \qquad \overset{\mathcal{D}_2}{k \in \mathcal{I}}}{\mathit{Safe}_n^{\mathcal{I},\mathcal{I}_\mu}(g)}[\text{safe}_1] \quad \Rightarrow \quad \dfrac{\dfrac{\overset{\mathcal{D}_{111}}{\mathcal{I}(l) = k} \qquad \overset{\mathcal{D}_{112}}{n \dot{-} k = g}}{n \dot{-} \mathcal{I}(l) = g}[\text{compute}_1]}{\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(l) = g}[\downarrow_1] \quad [\text{safe·image}]}[\&1]$$

$$\frac{\begin{array}{c} \overset{\mathcal{D}_1}{\mathit{Safe}_n^{\mathcal{I},\mathcal{I}_\mu}(t')} \quad \Rightarrow \quad \overset{\mathcal{D}_{11}}{\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(t) = t'} \quad [\text{safe·image}] \\ \overset{\mathcal{D}_2}{\mathit{Safe}_n^{\mathcal{I},\mathcal{I}_\mu}(u')} \quad \Rightarrow \quad \overset{\mathcal{D}_{12}}{\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(u) = u'} \quad [\text{safe·image}] \end{array}}{\dfrac{\overset{\mathcal{D}_1}{\mathit{Safe}_n^{\mathcal{I},\mathcal{I}_\mu}(t')} \qquad \overset{\mathcal{D}_2}{\mathit{Safe}_n^{\mathcal{I},\mathcal{I}_\mu}(u')}}{\mathit{Safe}_n^{\mathcal{I},\mathcal{I}_\mu}(t'\,u')}[\text{safe}_2] \quad \Rightarrow \quad \dfrac{\overset{\mathcal{D}_{11}}{\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(t) = t'} \qquad \overset{\mathcal{D}_{12}}{\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(u) = u'}}{\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(t\,u) = t'\,u'}[\downarrow_2] \quad [\text{safe·image}]}[\&2]$$

$$\frac{\overset{\mathcal{D}_1}{\mathit{Safe}_{n+1}^{(n+1::\mathcal{I}),\mathcal{I}_\mu}(t')} \quad \Rightarrow \quad \overset{\mathcal{D}_{11}}{\downarrow_{n+1}^{(n+1::\mathcal{I}),\mathcal{I}_\mu}(t) = t'} \quad [\text{safe·image}]}{\dfrac{\overset{\mathcal{D}_1}{\mathit{Safe}_{n+1}^{(n+1::\mathcal{I}),\mathcal{I}_\mu}(t')}}{\mathit{Safe}_n^{\mathcal{I},\mathcal{I}_\mu}(\lambda t')}[\text{safe}_3] \quad \Rightarrow \quad \dfrac{\overset{\mathcal{D}_{11}}{\downarrow_{n+1}^{(n+1::\mathcal{I}),\mathcal{I}_\mu}(t) = t'}}{\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(\lambda t) = \lambda t'}[\downarrow_3] \quad [\text{safe·image}]}[\&3]$$

$$\frac{\overset{\mathcal{D}_1}{\mathit{Safe}_n^{\mathcal{I},(\mathcal{I}::\mathcal{I}_\mu)}(t')} \quad \Rightarrow \quad \overset{\mathcal{D}_{11}}{\downarrow_n^{\mathcal{I},(\mathcal{I}::\mathcal{I}_\mu)}(t) = t'} \quad [\text{safe·image}]}{\dfrac{\overset{\mathcal{D}_1}{\mathit{Safe}_n^{\mathcal{I},(\mathcal{I}::\mathcal{I}_\mu)}(t')}}{\mathit{Safe}_n^{\mathcal{I},\mathcal{I}_\mu}(\mathbf{catch}\,t')}[\text{safe}_4] \quad \Rightarrow \quad \dfrac{\overset{\mathcal{D}_{11}}{\downarrow_n^{\mathcal{I},(\mathcal{I}::\mathcal{I}_\mu)}(t) = t'}}{\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(\textbf{get-context}\,t) = \mathbf{catch}\,t'}[\downarrow_4] \quad [\text{safe·image}]}[\&4]$$

$$\frac{\overset{\mathcal{D}_2}{\mathit{Safe}_n^{\mathcal{I}',\mathcal{I}_\mu}(t')} \quad \Rightarrow \quad \overset{\mathcal{D}_{12}}{\downarrow_n^{\mathcal{I}',\mathcal{I}_\mu}(t) = t'} \quad [\text{safe·image}]}{\dfrac{\overset{\mathcal{D}_{11}}{\mathcal{I}_\mu(\alpha) = \mathcal{I}'} \qquad \overset{\mathcal{D}_2}{\mathit{Safe}_n^{\mathcal{I}',\mathcal{I}_\mu}(t')}}{\mathit{Safe}_n^{\mathcal{I},\mathcal{I}_\mu}(\mathbf{throw}\,\alpha\,t')}[\text{safe}_5] \quad \Rightarrow \quad \dfrac{\overset{\mathcal{D}_{11}}{\mathcal{I}_\mu(\alpha) = \mathcal{I}'} \qquad \overset{\mathcal{D}_{12}}{\downarrow_n^{\mathcal{I}',\mathcal{I}_\mu}(t) = t'}}{\downarrow_n^{\mathcal{I},\mathcal{I}_\mu}(\textbf{set-context}\,\alpha\,t) = \mathbf{throw}\,\alpha\,t'}[\downarrow_5] \quad [\text{safe·image}]}[\&5]$$

%mode $+\mathcal{D}_1 \quad \Rightarrow \quad -\mathcal{D}_2$ [safe·image]
%worlds $() \quad \mathcal{D}_1 \quad \Rightarrow \quad \mathcal{D}_2$ [safe·image]
%total $(\mathcal{D}_1) \quad \mathcal{D}_1 \quad \Rightarrow \quad \mathcal{D}_2$ [safe·image] □

2.3 Examples

$1 \;=\; 0+1.$
$2 \;=\; 1+1.$
$3 \;=\; 2+1.$

%solve _ : $\mathit{Safe}_0^{[],[]}(\lambda \mathbf{catch}\,\lambda(0\,(\mathbf{throw}\,0\,1)))$

Remark. This example fails as expected:
%solve _ : $\mathit{Safe}_0^{[],[]}(\lambda \mathbf{catch}\,\lambda(1\,(\mathbf{throw}\,0\,0)))$

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

%solve d_1 : $\mathit{Safe}_0^{[],[]}(\lambda \mathbf{catch}\,\lambda(0\,(\mathbf{throw}\,0\,1)))$

%solve _ : $d_1\colon \mathit{Safe}_0^{[],[]}(\lambda \mathbf{catch}\,\lambda(0\,(\mathbf{throw}\,0\,1))) \quad \Rightarrow \quad \mathcal{D}_2\colon \downarrow_0^{[],[]}(t) = \lambda \mathbf{catch}\,\lambda(0\,(\mathbf{throw}\,0\,1))$ [safe·image]

%query 0 * $\mathit{Safe}_0^{[],[]}(\lambda \mathbf{catch}\,\lambda(1\,(\mathbf{throw}\,0\,0)))$
%query 1 * $\mathit{Safe}_0^{[],[]}(\lambda \mathbf{catch}\,\lambda(0\,(\mathbf{throw}\,0\,1)))$

%query 1 * $d_1\colon \mathit{Safe}_0^{[],[]}(\lambda \mathbf{catch}\,\lambda(0\,(\mathbf{throw}\,0\,1))) \quad \Rightarrow \quad \mathcal{D}_2\colon \downarrow_0^{[],[]}(t) = \lambda \mathbf{catch}\,\lambda(0\,(\mathbf{throw}\,0\,1))$ [safe·image]

Remark.