# Destination $\lambda$-calculus

Thomas Bagrel

April 17, 2024

## 1 Term and value syntax

| | | | |
|---|---|---|---|
| var, x, y | Term-level variable name | | |
| k | Index for ranges | | |

| | | | |
|---|---|---|---|
| hvar, h | ::= | | Hole or destination name ($\mathbb{N}$) |
| | $\mathtt{h}+\mathtt{h}'$ | M | |
| | $\mathtt{h}[\mathtt{H}\pm\mathtt{h}']$ | M | Shift by $\mathtt{h}'$ if $\mathtt{h} \in \mathtt{H}$ |
| | $\mathtt{max}(\mathtt{H})$ | M | Maximum of a set of holes |

| | | | |
|---|---|---|---|
| hvars, H | ::= | | Set of hole names |
| | $\{\mathtt{h}_1, .., \mathtt{h}_k\}$ | | |
| | $\mathtt{H}_1 \cup \mathtt{H}_2$ | M | Union of sets |
| | $\mathtt{H}\pm\mathtt{h}'$ | M | Shift all names from H by $\mathtt{h}'$. |
| | $\mathtt{hvars}(\Gamma)$ | M | Hole names of a context (requires $\mathtt{ctx\_NoVar}(\Gamma)$) |
| | $\mathtt{hvars}(\mathsf{C})$ | M | Hole names of an evaluation context |

| | | | |
|---|---|---|---|
| term, t, u | ::= | | Term |
| | v | | Value |
| | x | | Variable |
| | $\mathsf{t} \succ \mathsf{t}'$ | | Application |
| | $\mathsf{t} \,;\, \mathsf{u}$ | | Pattern-match on unit |
| | $\mathsf{t} \succ \mathsf{case}_m \{ \mathsf{Inl}\, \mathsf{x}_1 \mapsto \mathsf{u}_1 \,,\ \mathsf{Inr}\, \mathsf{x}_2 \mapsto \mathsf{u}_2 \}$ | | Pattern-match on sum |
| | $\mathsf{t} \succ \mathsf{case}_m (\mathsf{x}_1 \,,\, \mathsf{x}_2) \mapsto \mathsf{u}$ | | Pattern-match on product |
| | $\mathsf{t} \succ \mathsf{case}_m \mathrm{E}^n\, \mathsf{x} \mapsto \mathsf{u}$ | | Pattern-match on exponential |
| | $\mathsf{t} \succ \mathsf{map}\ \mathsf{x} \mapsto \mathsf{t}'$ | | Map over the right side of ampar t |
| | $\mathsf{to}_{\ltimes}\ \mathsf{u}$ | | Wrap u into a trivial ampar |
| | $\mathsf{from}_{\ltimes}\ \mathsf{t}$ | | Extract value from trivial ampar |
| | $\mathsf{t} \lhd ()$ | | Fill destination with unit |
| | $\mathsf{t} \lhd \mathsf{Inl}$ | | Fill destination with left variant |
| | $\mathsf{t} \lhd \mathsf{Inr}$ | | Fill destination with right variant |
| | $\mathsf{t} \lhd \mathrm{E}^m$ | | Fill destination with exponential constructor |
| | $\mathsf{t} \lhd (,)$ | | Fill destination with product constructor |
| | $\mathsf{t} \lhd (\lambda \mathsf{x}_m \mapsto \mathsf{u})$ | | Fill destination with function |
| | $\mathsf{t} \lhd_\bullet \mathsf{t}'$ | | Fill destination with root of ampar t′ |
| | $\mathsf{t}[\mathsf{x} := \mathsf{v}]$ | M | |

| | | | |
|---|---|---|---|
| val, v | ::= | | Term value |
| | $-\mathtt{h}$ | | Hole |
| | $+\mathtt{h}$ | | Destination |
| | $()$ | | Unit |
| | $\lambda^{\mathsf{v}} \mathsf{x}_m \mapsto \mathsf{u}$ | | Lambda abstraction |
| | $\mathsf{Inl}\, \mathsf{v}$ | | Left variant for sum |
| | $\mathsf{Inr}\, \mathsf{v}$ | | Right variant for sum |
| | $\mathrm{E}^m\, \mathsf{v}$ | | Exponential |
| | $(\mathsf{v}_1 \,,\, \mathsf{v}_2)$ | | Product |
| | $_{\mathtt{H}}\langle \mathsf{v}_2 \,,\, \mathsf{v}_1 \rangle$ | | Ampar |
| | $\mathsf{v}[\mathtt{H}\pm\mathtt{h}']$ | M | Shift hole names inside v by $\mathtt{h}'$ if they belong to H. |

| | | | | |
|---|---|---|---|---|
| ectx, c | ::= | | | Evaluation context component |
| | \| | $\square \succ t'$ | | Application |
| | \| | $v \succ \square$ | | Application |
| | \| | $\square \,;\, u$ | | Pattern-match on unit |
| | \| | $\square \succ \mathsf{case}_m \{ \mathsf{Inl}\, x_1 \mapsto u_1 \,,\ \mathsf{Inr}\, x_2 \mapsto u_2 \}$ | | Pattern-match on sum |
| | \| | $\square \succ \mathsf{case}_m (x_1 \,, x_2) \mapsto u$ | | Pattern-match on product |
| | \| | $\square \succ \mathsf{case}_m \, \mathrm{E}^n \, x \mapsto u$ | | Pattern-match on exponential |
| | \| | $\square \succ \mathsf{map}\ x \mapsto t'$ | | Map over the right side of ampar |
| | \| | $\mathsf{to}_{\ltimes}\ \square$ | | Wrap into a trivial ampar |
| | \| | $\mathsf{from}_{\ltimes}\ \square$ | | Extract value from trivial ampar |
| | \| | $\square \triangleleft ()$ | | Fill destination with unit |
| | \| | $\square \triangleleft \mathsf{Inl}$ | | Fill destination with left variant |
| | \| | $\square \triangleleft \mathsf{Inr}$ | | Fill destination with right variant |
| | \| | $\square \triangleleft \mathrm{E}^m$ | | Fill destination with exponential constructor |
| | \| | $\square \triangleleft (,)$ | | Fill destination with product constructor |
| | \| | $\square \triangleleft (\lambda x \,_m \mapsto u)$ | | Fill destination with function |
| | \| | $\square \triangleleft_\bullet t'$ | | Fill destination with root of ampar |
| | \| | $v \triangleleft_\bullet \square$ | | Fill destination with root of ampar |
| | \| | $\overset{\mathrm{op}}{\mathtt{H}}\langle v_2 \,, \square$ | | Open ampar. Only new addition to term shapes |
| ectxs, C | ::= | | | Evaluation context stack |
| | \| | $\square$ | | Represent the empty stack / "identity" evaluation context |
| | \| | $C \circ c$ | | Push c on top of C |
| | \| | $C[\mathtt{h} :=_{\mathtt{H}} v]$ | M | Fill h in C with value v (that may contain holes) |

## 2 Type system

| | | | | |
|---|---|---|---|---|
| type, T, U | ::= | | | Type |
| | \| | $\mathbf{1}$ | | Unit |
| | \| | $\mathbf{T}_1 \oplus \mathbf{T}_2$ | | Sum |
| | \| | $\mathbf{T}_1 \otimes \mathbf{T}_2$ | | Product |
| | \| | $!^m \mathbf{T}$ | | Exponential |
| | \| | $\mathbf{U} \ltimes \mathbf{T}$ | | Ampar type (consuming T yields U) |
| | \| | $\mathbf{T} \,_m\!\!\rightarrow \mathbf{U}$ | | Function |
| | \| | $\lfloor \mathbf{T} \rfloor^m$ | | Destination |
| *mode*, $m$, $n$ | ::= | | | Mode (Semiring) |
| | \| | $pa$ | | Pair of a multiplicity and age |
| | \| | $☠$ | | Error case (incompatible types, multiplicities, or ages) |
| | \| | $m_1 \cdot \ldots \cdot m_k$ | M | Semiring product |
| *mul*, $p$ | ::= | | | Multiplicity (first component of modality) |
| | \| | $1$ | | Linear. Neutral element of the product |
| | \| | $\omega$ | | Non-linear. Absorbing for the product |
| | \| | $p_1 \cdot \ldots \cdot p_k$ | M | Semiring product |
| *age*, $a$ | ::= | | | Age (second component of modality) |
| | \| | $\nu$ | | Born now. Neutral element of the product |
| | \| | $\uparrow$ | | One scope older |
| | \| | $\infty$ | | Infinitely old / static. Absorbing for the product |
| | \| | $a_1 \cdot \ldots \cdot a_k$ | M | Semiring product |
| ctx, $\Gamma$, $\Delta$, $\Pi$ | ::= | | | Typing context |
| | \| | $\{x :\, _m \mathbf{T}\}$ | | |
| | \| | $\{+\mathtt{h} :\, _m \lfloor \mathbf{T} \rfloor^n\}$ | | |
| | \| | $\{-\mathtt{h} : \mathbf{T}^n\}$ | | |
| | \| | $m \cdot \Gamma$ | M | Multiply each binding by $m$ |
| | \| | $\Gamma_1 \uplus \Gamma_2$ | M | Sum contexts $\Gamma_1$ and $\Gamma_2$. Duplicate keys with incompatible values will be tagged |
| | \| | $-\Gamma$ | M | Transforms dest bindings into a hole bindings (requires `ctx_DestOnly` $\Gamma$ and `ctx` |
| | \| | $-^{-1}\Gamma$ | M | Transforms hole bindings into dest bindings with left mode $1\nu$ (requires `ctx_Hol` |

| $\Gamma[\mathtt{H}{\pm}\mathtt{h}']$ M  Shift hole/dest names by $\mathtt{h}'$ if they belong to $\mathtt{H}$

$\boxed{\Gamma \Vdash \mathsf{v} : \mathsf{T}}$ *(Typing of values (raw))*

TyR-val-H
$$\frac{}{\{-\mathtt{h} : \mathsf{T}^{\mathit{1}\nu}\} \Vdash -\mathtt{h} : \mathsf{T}}$$

TyR-val-D
$$\frac{}{\{+\mathtt{h} : {}_{\mathit{1}\nu}\lfloor \mathsf{T} \rfloor^{n}\} \Vdash +\mathtt{h} : \lfloor \mathsf{T} \rfloor^{n}}$$

TyR-val-U
$$\frac{}{\{\} \Vdash () : \mathsf{1}}$$

TyR-val-F
$$\frac{\mathtt{IsValid}\ m \qquad \mathtt{DestOnly}\ \Delta \qquad \Delta \uplus \{\mathsf{x} : {}_{m}\mathsf{T}\} \vdash \mathsf{u} : \mathsf{U}}{\Delta \Vdash \lambda^{\mathsf{v}} \mathsf{x}\ {}_{m}\mapsto \mathsf{u} : \mathsf{T}\ {}_{m}{\to}\ \mathsf{U}}$$

TyR-val-L
$$\frac{\Gamma \Vdash \mathsf{v}_1 : \mathsf{T}_1}{\Gamma \Vdash \mathsf{Inl}\, \mathsf{v}_1 : \mathsf{T}_1 \oplus \mathsf{T}_2}$$

TyR-val-R
$$\frac{\Gamma \Vdash \mathsf{v}_2 : \mathsf{T}_2}{\Gamma \Vdash \mathsf{Inr}\, \mathsf{v}_2 : \mathsf{T}_1 \oplus \mathsf{T}_2}$$

TyR-val-P
$$\frac{\Gamma_1 \Vdash \mathsf{v}_1 : \mathsf{T}_1 \qquad \Gamma_2 \Vdash \mathsf{v}_2 : \mathsf{T}_2}{\Gamma_1 \uplus \Gamma_2 \Vdash (\mathsf{v}_1\, ,\, \mathsf{v}_2) : \mathsf{T}_1 \otimes \mathsf{T}_2}$$

TyR-val-E
$$\frac{\Gamma \Vdash \mathsf{v}' : \mathsf{T} \qquad \mathtt{IsValid}\ n}{n{\cdot}\Gamma \Vdash \mathrm{E}^{n}\, \mathsf{v}' : !^{n}\, \mathsf{T}}$$

TyR-val-A
$$\frac{\begin{array}{c}\mathtt{DestOnly}\ \Delta_1 \\ \mathtt{DestOnly}\ \Delta_2 \qquad \mathtt{DestOnly}\ \Delta_3 \\ \mathtt{LinOnly}\ \Delta_3 \qquad \mathtt{FinAgeOnly}\ \Delta_3 \\ \mathtt{ValidOnly}\ \Delta_3 \\ \Delta_1\ \#\ \Delta_2 \qquad \Delta_1\ \#\ \Delta_3 \\ \Delta_2\ \#\ \Delta_3 \qquad \mathit{1}{\uparrow}{\cdot}\Delta_1 \uplus \Delta_3 \Vdash \mathsf{v}_1 : \mathsf{T} \\ \Delta_2 \uplus (-\Delta_3) \Vdash \mathsf{v}_2 : \mathsf{U}\end{array}}{\Delta_1 \uplus \Delta_2 \Vdash {}_{\mathtt{hvars}(-\Delta_3)}\langle \mathsf{v}_2\, ,\, \mathsf{v}_1 \rangle : \mathsf{U} \ltimes \mathsf{T}}$$

$\boxed{\Pi \vdash \mathsf{t} : \mathsf{T}}$ *(Typing of terms)*

Ty-term-Val
$$\frac{\begin{array}{c}\mathtt{DestOnly}\ \Delta \\ \mathtt{DisposableOnly}\ \Pi \qquad \Delta \Vdash \mathsf{v} : \mathsf{T}\end{array}}{\Pi \uplus \Delta \vdash \mathsf{v} : \mathsf{T}}$$

Ty-term-Var
$$\frac{\begin{array}{c}\mathtt{DisposableOnly}\ \Pi \\ \Pi\ \#\ \{\mathsf{x} : {}_{m}\mathsf{T}\} \\ \mathtt{ModeSubtype}\ m\ \mathit{1}\nu\end{array}}{\Pi \uplus \{\mathsf{x} : {}_{m}\mathsf{T}\} \vdash \mathsf{x} : \mathsf{T}}$$

Ty-term-App
$$\frac{\mathtt{IsValid}\ m \qquad \Pi_1 \vdash \mathsf{t} : \mathsf{T} \qquad \Pi_2 \vdash \mathsf{t}' : \mathsf{T}\ {}_{m}{\to}\ \mathsf{U}}{m{\cdot}\Pi_1 \uplus \Pi_2 \vdash \mathsf{t} \succ \mathsf{t}' : \mathsf{U}}$$

Ty-term-PatU
$$\frac{\Pi_1 \vdash \mathsf{t} : \mathsf{1} \qquad \Pi_2 \vdash \mathsf{u} : \mathsf{U}}{\Pi_1 \uplus \Pi_2 \vdash \mathsf{t}\ ;\ \mathsf{u} : \mathsf{U}}$$

Ty-term-PatS
$$\frac{\begin{array}{c}\mathtt{IsValid}\ m \qquad \Pi_2\ \#\ \{\mathsf{x}_1 : {}_{m}\mathsf{T}_1\} \\ \Pi_2\ \#\ \{\mathsf{x}_2 : {}_{m}\mathsf{T}_2\} \\ \Pi_1 \vdash \mathsf{t} : \mathsf{T}_1 \oplus \mathsf{T}_2 \\ \Pi_2 \uplus \{\mathsf{x}_1 : {}_{m}\mathsf{T}_1\} \vdash \mathsf{u}_1 : \mathsf{U} \\ \Pi_2 \uplus \{\mathsf{x}_2 : {}_{m}\mathsf{T}_2\} \vdash \mathsf{u}_2 : \mathsf{U}\end{array}}{m{\cdot}\Pi_1 \uplus \Pi_2 \vdash \mathsf{t} \succ \mathsf{case}_{m}\, \{\, \mathsf{Inl}\, \mathsf{x}_1 \mapsto \mathsf{u}_1\, ,\ \mathsf{Inr}\, \mathsf{x}_2 \mapsto \mathsf{u}_2\, \} : \mathsf{U}}$$

Ty-term-PatP
$$\frac{\begin{array}{c}\mathtt{IsValid}\ m \qquad \Pi_2\ \#\ \{\mathsf{x}_1 : {}_{m}\mathsf{T}_1\} \\ \Pi_2\ \#\ \{\mathsf{x}_2 : {}_{m}\mathsf{T}_2\} \\ \{\mathsf{x}_1 : {}_{m}\mathsf{T}_1\}\ \#\ \{\mathsf{x}_2 : {}_{m}\mathsf{T}_2\} \\ \Pi_1 \vdash \mathsf{t} : \mathsf{T}_1 \otimes \mathsf{T}_2 \\ \Pi_2 \uplus \{\mathsf{x}_1 : {}_{m}\mathsf{T}_1\} \uplus \{\mathsf{x}_2 : {}_{m}\mathsf{T}_2\} \vdash \mathsf{u} : \mathsf{U}\end{array}}{m{\cdot}\Pi_1 \uplus \Pi_2 \vdash \mathsf{t} \succ \mathsf{case}_{m}\, (\mathsf{x}_1\, ,\, \mathsf{x}_2) \mapsto \mathsf{u} : \mathsf{U}}$$

Ty-term-PatE
$$\frac{\begin{array}{c}\mathtt{IsValid}\ m \qquad \mathtt{IsValid}\ n \\ \Pi_2\ \#\ \{\mathsf{x} : {}_{m{\cdot}n}\mathsf{T}\} \qquad \Pi_1 \vdash \mathsf{t} : !^{n}\, \mathsf{T} \\ \Pi_2 \uplus \{\mathsf{x} : {}_{m{\cdot}n}\mathsf{T}\} \vdash \mathsf{u} : \mathsf{U}\end{array}}{m{\cdot}\Pi_1 \uplus \Pi_2 \vdash \mathsf{t} \succ \mathsf{case}_{m}\, \mathrm{E}^{n}\, \mathsf{x} \mapsto \mathsf{u} : \mathsf{U}}$$

Ty-term-Map
$$\frac{\Pi_2\ \#\ \{\mathsf{x} : {}_{\mathit{1}\nu}\mathsf{T}\} \qquad \Pi_1 \vdash \mathsf{t} : \mathsf{U} \ltimes \mathsf{T} \qquad \mathit{1}{\uparrow}{\cdot}\Pi_2 \uplus \{\mathsf{x} : {}_{\mathit{1}\nu}\mathsf{T}\} \vdash \mathsf{t}' : \mathsf{T}'}{\Pi_1 \uplus \Pi_2 \vdash \mathsf{t} \succ \mathsf{map}\ \mathsf{x} \mapsto \mathsf{t}' : \mathsf{U} \ltimes \mathsf{T}'}$$

Ty-term-ToA
$$\frac{\Pi \vdash \mathsf{u} : \mathsf{U}}{\Pi \vdash \mathsf{to}_{\ltimes}\, \mathsf{u} : \mathsf{U} \ltimes \mathsf{1}}$$

Ty-term-FromA
$$\frac{\Pi \vdash \mathsf{t} : \mathsf{U} \ltimes \mathsf{1}}{\Pi \vdash \mathsf{from}_{\ltimes}\, \mathsf{t} : \mathsf{U}}$$

Ty-term-FillU
$$\frac{\Pi \vdash \mathsf{t} : \lfloor \mathsf{1} \rfloor^{n}}{\Pi \vdash \mathsf{t} \triangleleft () : \mathsf{1}}$$

Ty-term-FillL
$$\frac{\Pi \vdash \mathsf{t} : \lfloor \mathsf{T}_1 \oplus \mathsf{T}_2 \rfloor^{n}}{\Pi \vdash \mathsf{t} \triangleleft \mathsf{Inl} : \lfloor \mathsf{T}_1 \rfloor^{n}}$$

Ty-term-FillR
$$\frac{\Pi \vdash \mathsf{t} : \lfloor \mathsf{T}_1 \oplus \mathsf{T}_2 \rfloor^{n}}{\Pi \vdash \mathsf{t} \triangleleft \mathsf{Inr} : \lfloor \mathsf{T}_2 \rfloor^{n}}$$

Ty-term-FillP
$$\frac{\Pi \vdash \mathsf{t} : \lfloor \mathsf{T}_1 \otimes \mathsf{T}_2 \rfloor^{n}}{\Pi \vdash \mathsf{t} \triangleleft (,) : \lfloor \mathsf{T}_1 \rfloor^{n} \otimes \lfloor \mathsf{T}_2 \rfloor^{n}}$$

Ty-term-FillE
$$\frac{\mathtt{IsValid}\ n \qquad \Pi \vdash \mathsf{t} : \lfloor !^{n'}\, \mathsf{T} \rfloor^{n}}{\Pi \vdash \mathsf{t} \triangleleft \mathrm{E}^{n'} : \lfloor \mathsf{T} \rfloor^{n'{\cdot}n}}$$

Ty-term-FillF
$$\frac{\begin{array}{c}\mathtt{IsValid}\ m \\ \mathtt{IsValid}\ n \qquad \Pi_2\ \#\ \{\mathsf{x} : {}_{m}\mathsf{T}\} \\ \Pi_1 \vdash \mathsf{t} : \lfloor \mathsf{T}\ {}_{m}{\to}\ \mathsf{U} \rfloor^{n} \\ \Pi_2 \uplus \{\mathsf{x} : {}_{m}\mathsf{T}\} \vdash \mathsf{u} : \mathsf{U}\end{array}}{\Pi_1 \uplus (\mathit{1}{\uparrow}{\cdot}n){\cdot}\Pi_2 \vdash \mathsf{t} \triangleleft (\lambda \mathsf{x}\ {}_{m}\mapsto \mathsf{u}) : \mathsf{1}}$$

Ty-term-FillC
$$\frac{\begin{array}{c}\mathtt{IsValid}\ n \\ \Pi_1 \vdash \mathsf{t} : \lfloor \mathsf{U} \rfloor^{n} \qquad \Pi_2 \vdash \mathsf{t}' : \mathsf{U} \ltimes \mathsf{T}\end{array}}{\Pi_1 \uplus (\mathit{1}{\uparrow}{\cdot}n){\cdot}\Pi_2 \vdash \mathsf{t} \triangleleft_{\bullet} \mathsf{t}' : \mathsf{T}}$$

$\boxed{\Delta \dashv C : T \rightarrowtail U_0}$ *(Typing of evaluation contexts)*

Ty-ectxs-Id
$$\frac{}{\{\} \dashv \Box : U_0 \rightarrowtail U_0}$$

Ty-ectxs-AppFoc1
$$\frac{\begin{array}{c}\Delta_1 \# \Delta_2 \\ \texttt{DestOnly}\ \Delta_1 \qquad \texttt{DestOnly}\ \Delta_2 \\ \texttt{IsValid}\ m \qquad \texttt{ValidOnly}\ \Delta_2 \\ m{\cdot}\Delta_1 \uplus \Delta_2 \dashv C : U \rightarrowtail U_0 \\ \Delta_2 \vdash t' : T \ {}_m\!\!\rightarrow U\end{array}}{\Delta_1 \dashv C \circ (\Box \succ t') : T \rightarrowtail U_0}$$

Ty-ectxs-AppFoc2
$$\frac{\begin{array}{c}\Delta_1 \# \Delta_2 \\ \texttt{DestOnly}\ \Delta_1 \qquad \texttt{DestOnly}\ \Delta_2 \\ \texttt{IsValid}\ m \qquad \texttt{ValidOnly}\ \Delta_1 \\ m{\cdot}\Delta_1 \uplus \Delta_2 \dashv C : U \rightarrowtail U_0 \\ \Delta_1 \vdash v : T\end{array}}{\Delta_2 \dashv C \circ (v \succ \Box) : (T \ {}_m\!\!\rightarrow U) \rightarrowtail U_0}$$

Ty-ectxs-PatSFoc
$$\frac{\begin{array}{c}\Delta_1 \# \Delta_2 \\ \texttt{DestOnly}\ \Delta_1 \qquad \texttt{DestOnly}\ \Delta_2 \\ \texttt{IsValid}\ m \qquad \texttt{ValidOnly}\ \Delta_2 \\ m{\cdot}\Delta_1 \uplus \Delta_2 \dashv C : U \rightarrowtail U_0 \\ \Delta_2 \uplus \{x_1 : {}_m T_1\} \vdash u_1 : U \\ \Delta_2 \uplus \{x_2 : {}_m T_2\} \vdash u_2 : U\end{array}}{\Delta_1 \dashv C \circ (\Box \succ \mathsf{case}_m \{\, \mathsf{Inl}\, x_1 \mapsto u_1 \,,\ \mathsf{Inr}\, x_2 \mapsto u_2 \,\}) : (T_1 \oplus T_2) \rightarrowtail U_0}$$

Ty-ectxs-PatUFoc
$$\frac{\begin{array}{c}\Delta_1 \# \Delta_2 \qquad \texttt{DestOnly}\ \Delta_1 \\ \texttt{DestOnly}\ \Delta_2 \qquad \texttt{ValidOnly}\ \Delta_2 \\ \Delta_1 \uplus \Delta_2 \dashv C : U \rightarrowtail U_0 \\ \Delta_2 \vdash u : U\end{array}}{\Delta_1 \dashv C \circ (\Box\ ;\ u) : 1 \rightarrowtail U_0}$$

Ty-ectxs-PatPFoc
$$\frac{\begin{array}{c}\Delta_1 \# \Delta_2 \\ \texttt{DestOnly}\ \Delta_1 \qquad \texttt{DestOnly}\ \Delta_2 \\ \{x_1 : {}_m T_1\} \# \{x_2 : {}_m T_2\} \\ \texttt{IsValid}\ m \qquad \texttt{ValidOnly}\ \Delta_2 \\ m{\cdot}\Delta_1 \uplus \Delta_2 \dashv C : U \rightarrowtail U_0 \\ \Delta_2 \uplus \{x_1 : {}_m T_1\} \uplus \{x_2 : {}_m T_2\} \vdash u : U\end{array}}{\Delta_1 \dashv C \circ (\Box \succ \mathsf{case}_m\, (x_1\,,\, x_2) \mapsto u) : (T_1 \otimes T_2) \rightarrowtail U_0}$$

Ty-ectxs-PatEFoc
$$\frac{\begin{array}{c}\Delta_1 \# \Delta_2 \qquad \texttt{DestOnly}\ \Delta_1 \\ \texttt{DestOnly}\ \Delta_2 \qquad \texttt{IsValid}\ m \\ \texttt{IsValid}\ m' \qquad \texttt{ValidOnly}\ \Delta_2 \\ m{\cdot}\Delta_1 \uplus \Delta_2 \dashv C : U \rightarrowtail U_0 \\ \Delta_2 \uplus \{x : {}_{m{\cdot}m'} T\} \vdash u : U\end{array}}{\Delta_1 \dashv C \circ (\Box \succ \mathsf{case}_m\, E^{m'}\, x \mapsto u) : !^{m'}\, T \rightarrowtail U_0}$$

Ty-ectxs-MapFoc
$$\frac{\begin{array}{c}\Delta_1 \# \Delta_2 \qquad \texttt{DestOnly}\ \Delta_1 \\ \texttt{DestOnly}\ \Delta_2 \qquad \texttt{ValidOnly}\ \Delta_2 \\ \Delta_1 \uplus \Delta_2 \dashv C : U \ltimes T' \rightarrowtail U_0 \\ 1\!\uparrow{\cdot}\Delta_2 \uplus \{x : {}_{1\nu} T\} \vdash t' : T'\end{array}}{\Delta_1 \dashv C \circ (\Box \succ \mathsf{map}\ x \mapsto t') : (U \ltimes T) \rightarrowtail U_0}$$

Ty-ectxs-ToAFoc
$$\frac{\Delta \dashv C : (U \ltimes 1) \rightarrowtail U_0}{\Delta \dashv C \circ (\mathsf{to}_\ltimes\, \Box) : U \rightarrowtail U_0}$$

Ty-ectxs-FromAFoc
$$\frac{\Delta \dashv C : U \rightarrowtail U_0}{\Delta \dashv C \circ (\mathsf{from}_\ltimes\, \Box) : (U \ltimes 1) \rightarrowtail U_0}$$

Ty-ectxs-FillUFoc
$$\frac{\Delta \dashv C : 1 \rightarrowtail U_0}{\Delta \dashv C \circ (\Box \triangleleft ()) : \lfloor 1 \rfloor^n \rightarrowtail U_0}$$

Ty-ectxs-FillLFoc
$$\frac{\Delta \dashv C : \lfloor T_1 \rfloor^n \rightarrowtail U_0}{\Delta \dashv C \circ (\Box \triangleleft \mathsf{Inl}) : \lfloor T_1 \oplus T_2 \rfloor^n \rightarrowtail U_0}$$

Ty-ectxs-FillRFoc
$$\frac{\Delta \dashv C : \lfloor T_2 \rfloor^n \rightarrowtail U_0}{\Delta \dashv C \circ (\Box \triangleleft \mathsf{Inr}) : \lfloor T_1 \oplus T_2 \rfloor^n \rightarrowtail U_0}$$

Ty-ectxs-FillFFoc
$$\frac{\begin{array}{c}\Delta_1 \# \Delta_2 \qquad \texttt{DestOnly}\ \Delta_1 \\ \texttt{DestOnly}\ \Delta_2 \qquad \texttt{ValidOnly}\ \Delta_2 \\ \texttt{IsValid}\ m \qquad \texttt{IsValid}\ n \\ \Delta_1 \uplus (1\!\uparrow{\cdot}n){\cdot}\Delta_2 \dashv C : 1 \rightarrowtail U_0 \\ \Delta_2 \uplus \{x : {}_m T\} \vdash u : U\end{array}}{\Delta_1 \dashv C \circ (\Box \triangleleft (\lambda x_{\,m} \mapsto u)) : \lfloor T \ {}_m\!\!\rightarrow U \rfloor^n \rightarrowtail U_0}$$

Ty-ectxs-FillPFoc
$$\frac{\Delta \dashv C : (\lfloor T_1 \rfloor^n \otimes \lfloor T_2 \rfloor^n) \rightarrowtail U_0}{\Delta \dashv C \circ (\Box \triangleleft (,)) : \lfloor T_1 \otimes T_2 \rfloor^n \rightarrowtail U_0}$$

Ty-ectxs-FillEFoc
$$\frac{\begin{array}{c}\texttt{IsValid}\ m \\ \Delta \dashv C : \lfloor T \rfloor^{m{\cdot}n} \rightarrowtail U_0\end{array}}{\Delta \dashv C \circ (\Box \triangleleft E^m) : \lfloor\!\lfloor^m T \rfloor^n \rightarrowtail U_0}$$

Ty-ectxs-AOpenFoc
$$\frac{\begin{array}{c}\Delta_1 \# \Delta_2 \\ \Delta_1 \# \Delta_3 \qquad \Delta_2 \# \Delta_3 \\ \mathsf{hvars}(C)\ \#\#\ \mathsf{hvars}(-\Delta_3) \\ \texttt{DestOnly}\ \Delta_1 \\ \texttt{DestOnly}\ \Delta_2 \qquad \texttt{DestOnly}\ \Delta_3 \\ \texttt{LinOnly}\ \Delta_3 \qquad \texttt{FinAgeOnly}\ \Delta_3 \\ \texttt{ValidOnly}\ \Delta_3 \\ \Delta_1 \uplus \Delta_2 \dashv C : (U \ltimes T') \rightarrowtail U_0 \\ \Delta_2 \uplus -\Delta_3 \Vdash v_2 : U\end{array}}{1\!\uparrow{\cdot}\Delta_1 \uplus \Delta_3 \dashv C \circ ({}^{\mathrm{op}}_{\mathsf{hvars}(-\Delta_3)}\langle v_2\,,\, \Box) : T' \rightarrowtail U_0}$$

Ty-ectxs-FillCFoc1
$$\frac{\begin{array}{c}\Delta_1 \# \Delta_2 \\ \texttt{DestOnly}\ \Delta_1 \qquad \texttt{DestOnly}\ \Delta_2 \\ \texttt{ValidOnly}\ \Delta_2 \qquad \texttt{IsValid}\ n \\ \Delta_1 \uplus (1\!\uparrow{\cdot}n){\cdot}\Delta_2 \dashv C : T \rightarrowtail U_0 \\ \Delta_2 \vdash t' : U \ltimes T\end{array}}{\Delta_1 \dashv C \circ (\Box \triangleleft\!\bullet\, t') : \lfloor U \rfloor^n \rightarrowtail U_0}$$

Ty-ectxs-FillCFoc2
$$\frac{\begin{array}{c}\Delta_1 \# \Delta_2 \\ \texttt{DestOnly}\ \Delta_1 \qquad \texttt{DestOnly}\ \Delta_2 \\ \texttt{ValidOnly}\ \Delta_1 \qquad \texttt{IsValid}\ n \\ \Delta_1 \uplus (1\!\uparrow{\cdot}n){\cdot}\Delta_2 \dashv C : T \rightarrowtail U_0 \\ \Delta_1 \vdash v : \lfloor U \rfloor^n\end{array}}{\Delta_2 \dashv C \circ (v \triangleleft\!\bullet\, \Box) : U \ltimes T \rightarrowtail U_0}$$

$\boxed{\vdash C[t] : T}$ *(Typing of extended terms (pair of evaluation context and term))*

Ty-eterm-ClosedEterm
$$\frac{\begin{array}{c}\texttt{ValidOnly}\ \Delta \qquad \texttt{DestOnly}\ \Delta \\ \Delta \dashv C : T \rightarrowtail U_0 \qquad \Delta \vdash t : T\end{array}}{\vdash C[t] : U_0}$$

# 3 Small-step semantics

$\boxed{C[t] \longrightarrow C'[t']}$ *(Small-step evaluation of terms using evaluation contexts)*

Sem-eterm-AppFoc1
$$\frac{\texttt{NotVal}\ t}{C[t \succ t'] \longrightarrow (C \circ (\square \succ t'))[t]}$$

Sem-eterm-AppUnfoc1
$$\frac{}{(C \circ (\square \succ t'))[v] \longrightarrow C[v \succ t']}$$

Sem-eterm-AppFoc2
$$\frac{\texttt{NotVal}\ t'}{C[v \succ t'] \longrightarrow (C \circ (v \succ \square))[t']}$$

Sem-eterm-AppUnfoc2
$$\frac{}{(C \circ (v \succ \square))[v'] \longrightarrow C[v \succ v']}$$

Sem-eterm-AppRed
$$\frac{}{C[v \succ (\lambda^{v} x_{\,m} \mapsto u)] \longrightarrow C[u[x := v]]}$$

Sem-eterm-PatUFoc
$$\frac{\texttt{NotVal}\ t}{C[t\ ;\ u] \longrightarrow (C \circ (\square\ ;\ u))[t]}$$

Sem-eterm-PatUUnfoc
$$\frac{}{(C \circ (\square\ ;\ u))[v] \longrightarrow C[v\ ;\ u]}$$

Sem-eterm-PatURed
$$\frac{}{C[()\ ;\ u] \longrightarrow C[u]}$$

Sem-eterm-PatSFoc
$$\frac{\texttt{NotVal}\ t}{C[t \succ \mathsf{case}_m\,\{\,\mathsf{Inl}\,x_1 \mapsto u_1\,,\ \mathsf{Inr}\,x_2 \mapsto u_2\,\}] \longrightarrow (C \circ (\square \succ \mathsf{case}_m\,\{\,\mathsf{Inl}\,x_1 \mapsto u_1\,,\ \mathsf{Inr}\,x_2 \mapsto u_2\,\}))[t]}$$

Sem-eterm-PatSUnfoc
$$\frac{}{(C \circ (\square \succ \mathsf{case}_m\,\{\,\mathsf{Inl}\,x_1 \mapsto u_1\,,\ \mathsf{Inr}\,x_2 \mapsto u_2\,\}))[v] \longrightarrow C[v \succ \mathsf{case}_m\,\{\,\mathsf{Inl}\,x_1 \mapsto u_1\,,\ \mathsf{Inr}\,x_2 \mapsto u_2\,\}]}$$

Sem-eterm-PatLRed
$$\frac{}{C[(\mathsf{Inl}\,v_1) \succ \mathsf{case}_m\,\{\,\mathsf{Inl}\,x_1 \mapsto u_1\,,\ \mathsf{Inr}\,x_2 \mapsto u_2\,\}] \longrightarrow C[u_1[x_1 := v_1]]}$$

Sem-eterm-PatRRed
$$\frac{}{C[(\mathsf{Inr}\,v_2) \succ \mathsf{case}_m\,\{\,\mathsf{Inl}\,x_1 \mapsto u_1\,,\ \mathsf{Inr}\,x_2 \mapsto u_2\,\}] \longrightarrow C[u_2[x_2 := v_2]]}$$

Sem-eterm-PatPFoc
$$\frac{\texttt{NotVal}\ t}{C[t \succ \mathsf{case}_m\,(x_1\,,\,x_2) \mapsto u] \longrightarrow (C \circ (\square \succ \mathsf{case}_m\,(x_1\,,\,x_2) \mapsto u))[t]}$$

Sem-eterm-PatPUnfoc
$$\frac{}{(C \circ (\square \succ \mathsf{case}_m\,(x_1\,,\,x_2) \mapsto u))[v] \longrightarrow C[v \succ \mathsf{case}_m\,(x_1\,,\,x_2) \mapsto u]}$$

Sem-eterm-PatPRed
$$\frac{}{C[(v_1\,,\,v_2) \succ \mathsf{case}_m\,(x_1\,,\,x_2) \mapsto u] \longrightarrow C[u[x_1 := v_1][x_2 := v_2]]}$$

Sem-eterm-PatEFoc
$$\frac{\texttt{NotVal}\ t}{C[t \succ \mathsf{case}_m\,\mathrm{E}^{n}\,x \mapsto u] \longrightarrow (C \circ (\square \succ \mathsf{case}_m\,\mathrm{E}^{n}\,x \mapsto u))[t]}$$

Sem-eterm-PatEUnfoc
$$\frac{}{(C \circ (\square \succ \mathsf{case}_m\,\mathrm{E}^{n}\,x \mapsto u))[v] \longrightarrow C[v \succ \mathsf{case}_m\,\mathrm{E}^{n}\,x \mapsto u]}$$

Sem-eterm-PatERed
$$\frac{}{C[\mathrm{E}^{n}\,v' \succ \mathsf{case}_m\,\mathrm{E}^{n}\,x \mapsto u] \longrightarrow C[u[x := v']]}$$

Sem-eterm-MapFoc
$$\frac{\texttt{NotVal}\ t}{C[t \succ \mathsf{map}\ x \mapsto t'] \longrightarrow (C \circ (\square \succ \mathsf{map}\ x \mapsto t'))[t]}$$

Sem-eterm-MapUnfoc
$$\frac{}{(C \circ (\square \succ \mathsf{map}\ x \mapsto t'))[v] \longrightarrow C[v \succ \mathsf{map}\ x \mapsto t']}$$

Sem-eterm-MapRedAOpenFoc
$$\frac{h' = \mathtt{max(hvars(C))+1}}{C[{}_{\mathrm{H}}\langle v_2\,,\,v_1\rangle \succ \mathsf{map}\ x \mapsto t'] \longrightarrow (C \circ ({}^{\mathrm{op}}_{\mathrm{H}\pm h'}\langle v_2[\mathrm{H}\pm h']\,,\,\square\rangle))[t'[x := v_1[\mathrm{H}\pm h']]]}$$

Sem-eterm-AOpenUnfoc
$$\frac{}{(C \circ {}^{\mathrm{op}}_{\mathrm{H}}\langle v_2\,,\,\square\rangle)[v_1] \longrightarrow C[{}_{\mathrm{H}}\langle v_2\,,\,v_1\rangle]}$$

Sem-eterm-ToAFoc
$$\frac{\texttt{NotVal}\ u}{C[\mathsf{to}_{\ltimes}\ u] \longrightarrow (C \circ (\mathsf{to}_{\ltimes}\ \square))[u]}$$

Sem-eterm-ToAUnfoc
$$\frac{}{(C \circ (\mathsf{to}_{\ltimes}\ \square))[v_2] \longrightarrow C[\mathsf{to}_{\ltimes}\ v_2]}$$

Sem-eterm-ToARed
$$\frac{}{C[\mathsf{to}_{\ltimes}\ v_2] \longrightarrow C[{}_{\{\,\}}\langle v_2\,,\,()\rangle]}$$

Sem-eterm-FromAFoc
$$\frac{\texttt{NotVal}\ t}{C[\mathsf{from}_{\ltimes}\ t] \longrightarrow (C \circ (\mathsf{from}_{\ltimes}\ \square))[t]}$$

Sem-eterm-FromAUnfoc
$$\frac{}{(C \circ (\mathsf{from}_{\ltimes}\ \square))[v] \longrightarrow C[\mathsf{from}_{\ltimes}\ v]}$$

Sem-eterm-FromARed
$$\frac{}{C[\mathsf{from}_{\ltimes}\ {}_{\{\,\}}\langle v_2\,,\,()\rangle] \longrightarrow C[v_2]}$$

Sem-eterm-FillUFoc
$$\frac{\texttt{NotVal}\ t}{C[t \triangleleft ()] \longrightarrow (C \circ (\square \triangleleft ()))[t]}$$

Sem-eterm-FillUUnfoc
$$\frac{}{(C \circ (\square \triangleleft ()))[v] \longrightarrow C[v \triangleleft ()]}$$

Sem-eterm-FillURed
$$\frac{}{C[+h \triangleleft ()] \longrightarrow C[h :=_{\{\,\}}\ ()][()]}$$

Sem-eterm-FillLFoc
$$\frac{\texttt{NotVal t}}{\mathsf{C}[\mathsf{t} \lhd \mathsf{Inl}] \longrightarrow (\mathsf{C} \circ (\Box \lhd \mathsf{Inl}))[\mathsf{t}]}$$

Sem-eterm-FillLUnfoc
$$\frac{}{(\mathsf{C} \circ (\Box \lhd \mathsf{Inl}))[\mathsf{v}] \longrightarrow \mathsf{C}[\mathsf{v} \lhd \mathsf{Inl}]}$$

Sem-eterm-FillLRed
$$\frac{\mathsf{h'} = \mathsf{max}(\mathsf{hvars}(\mathsf{C}) \cup \{\mathsf{h}\}) + 1}{\mathsf{C}[+\mathsf{h} \lhd \mathsf{Inl}] \longrightarrow \mathsf{C}[\mathsf{h} :=_{\{\mathsf{h'}+1\}} \mathsf{Inl}\, -(\mathsf{h'}+1)][+(\mathsf{h'}+1)]}$$

Sem-eterm-FillRFoc
$$\frac{\texttt{NotVal t}}{\mathsf{C}[\mathsf{t} \lhd \mathsf{Inr}] \longrightarrow (\mathsf{C} \circ (\Box \lhd \mathsf{Inr}))[\mathsf{t}]}$$

Sem-eterm-FillRUnfoc
$$\frac{}{(\mathsf{C} \circ (\Box \lhd \mathsf{Inr}))[\mathsf{v}] \longrightarrow \mathsf{C}[\mathsf{v} \lhd \mathsf{Inr}]}$$

Sem-eterm-FillRRed
$$\frac{\mathsf{h'} = \mathsf{max}(\mathsf{hvars}(\mathsf{C}) \cup \{\mathsf{h}\}) + 1}{\mathsf{C}[+\mathsf{h} \lhd \mathsf{Inr}] \longrightarrow \mathsf{C}[\mathsf{h} :=_{\{\mathsf{h'}+1\}} \mathsf{Inr}\, -(\mathsf{h'}+1)][+(\mathsf{h'}+1)]}$$

Sem-eterm-FillEFoc
$$\frac{\texttt{NotVal t}}{\mathsf{C}[\mathsf{t} \lhd \mathrm{E}^{m}] \longrightarrow (\mathsf{C} \circ (\Box \lhd \mathrm{E}^{m}))[\mathsf{t}]}$$

Sem-eterm-FillEUnfoc
$$\frac{}{(\mathsf{C} \circ (\Box \lhd \mathrm{E}^{m}))[\mathsf{v}] \longrightarrow \mathsf{C}[\mathsf{v} \lhd \mathrm{E}^{m}]}$$

Sem-eterm-FillERed
$$\frac{\mathsf{h'} = \mathsf{max}(\mathsf{hvars}(\mathsf{C}) \cup \{\mathsf{h}\}) + 1}{\mathsf{C}[+\mathsf{h} \lhd \mathrm{E}^{m}] \longrightarrow \mathsf{C}[\mathsf{h} :=_{\{\mathsf{h'}+1\}} \mathrm{E}^{m}\, -(\mathsf{h'}+1)][+(\mathsf{h'}+1)]}$$

Sem-eterm-FillPFoc
$$\frac{\texttt{NotVal t}}{\mathsf{C}[\mathsf{t} \lhd (,)] \longrightarrow (\mathsf{C} \circ (\Box \lhd (,)))[\mathsf{t}]}$$

Sem-eterm-FillPUnfoc
$$\frac{}{(\mathsf{C} \circ (\Box \lhd (,)))[\mathsf{v}] \longrightarrow \mathsf{C}[\mathsf{v} \lhd (,)]}$$

Sem-eterm-FillPRed
$$\frac{\mathsf{h'} = \mathsf{max}(\mathsf{hvars}(\mathsf{C}) \cup \{\mathsf{h}\}) + 1}{\mathsf{C}[+\mathsf{h} \lhd (,)] \longrightarrow \mathsf{C}[\mathsf{h} :=_{\{\mathsf{h'}+1, \mathsf{h'}+2\}} (-(\mathsf{h'}+1), -(\mathsf{h'}+2))][(+(\mathsf{h'}+1), +(\mathsf{h'}+2))]}$$

Sem-eterm-FillFFoc
$$\frac{\texttt{NotVal t}}{\mathsf{C}[\mathsf{t} \lhd (\lambda \mathsf{x}_{\,m} \mapsto \mathsf{u})] \longrightarrow (\mathsf{C} \circ (\Box \lhd (\lambda \mathsf{x}_{\,m} \mapsto \mathsf{u})))[\mathsf{t}]}$$

Sem-eterm-FillFUnfoc
$$\frac{}{(\mathsf{C} \circ (\Box \lhd (\lambda \mathsf{x}_{\,m} \mapsto \mathsf{u})))[\mathsf{v}] \longrightarrow \mathsf{C}[\mathsf{v} \lhd (\lambda \mathsf{x}_{\,m} \mapsto \mathsf{u})]}$$

Sem-eterm-FillFRed
$$\frac{}{\mathsf{C}[+\mathsf{h} \lhd (\lambda \mathsf{x}_{\,m} \mapsto \mathsf{u})] \longrightarrow \mathsf{C}[\mathsf{h} :=_{\{\}} \lambda^{\mathsf{v}} \mathsf{x}_{\,m} \mapsto \mathsf{u}][()]}$$

Sem-eterm-FillCFoc1
$$\frac{\texttt{NotVal t}}{\mathsf{C}[\mathsf{t} \lhd_{\bullet} \mathsf{t'}] \longrightarrow (\mathsf{C} \circ (\Box \lhd_{\bullet} \mathsf{t'}))[\mathsf{t}]}$$

Sem-eterm-FillCUnfoc1
$$\frac{}{(\mathsf{C} \circ (\Box \lhd_{\bullet} \mathsf{t'}))[\mathsf{v}] \longrightarrow \mathsf{C}[\mathsf{v} \lhd_{\bullet} \mathsf{t'}]}$$

Sem-eterm-FillCFoc2
$$\frac{\texttt{NotVal t'}}{\mathsf{C}[\mathsf{v} \lhd_{\bullet} \mathsf{t'}] \longrightarrow (\mathsf{C} \circ (\mathsf{v} \lhd_{\bullet} \Box))[\mathsf{t'}]}$$

Sem-eterm-FillCUnfoc2
$$\frac{}{(\mathsf{C} \circ (\mathsf{v} \lhd_{\bullet} \Box))[\mathsf{v'}] \longrightarrow \mathsf{C}[\mathsf{v} \lhd_{\bullet} \mathsf{v'}]}$$

Sem-eterm-FillCRed
$$\frac{\mathsf{h'} = \mathsf{max}(\mathsf{hvars}(\mathsf{C}) \cup \{\mathsf{h}\}) + 1}{\mathsf{C}[+\mathsf{h} \lhd_{\bullet \mathrm{H}} \langle \mathsf{v}_2 \,,\, \mathsf{v}_1 \rangle] \longrightarrow \mathsf{C}[\mathsf{h} :=_{(\mathrm{H} \pm \mathsf{h'})} \mathsf{v}_2[\mathrm{H} \pm \mathsf{h'}]][\mathsf{v}_1[\mathrm{H} \pm \mathsf{h'}]]}$$

# 4 Remarks on the Coq proofs

- Not particularly elegant. Max number of goals observed 232 (solved by a single call to the `congruence` tactic). When you have a computer, brute force is a viable strategy. (in particular, no semiring formalisation, it was quicker to do directly)
- Rules generated by ott, same as in the article (up to some notational difference). Contexts are not generated purely by syntax, and are interpreted in a semantic domain (finite functions).
- Reasoning on closed terms avoids almost all complications on binder manipulation. Makes proofs tractable.
- Finite functions: making a custom library was less headache than using existing libraries (including `MMap`). Existing libraries don't provide some of the tools that we needed, but the most important factor ended up being the need for a modicum of dependency between key and value. There wasn't really that out there. Backed by actual functions for simplicity; cost: equality is complicated.
- Most of the proofs done by author with very little prior experience to Coq.
- Did proofs in Coq because context manipulations are tricky.
- Context sum made total by adding an extra invalid *mode* (rather than an extra context). It seems to be much simpler this way.
- It might be a good idea to provide statistics on the number of lemmas and size of Coq codebase.
- (possibly) renaming as permutation, inspired by nominal sets, make more lemmas don't require a condition (but some lemmas that wouldn't in a straight renaming do in exchange).
- (possibly) methodology: assume a lot of lemmas, prove main theorem, prove assumptions, some wrong, fix. A number of wrong lemma initially assumed, but replacing them by correct variant was always easy to fix in proofs.
- Axioms that we use and why (in particular setoid equality not very natural with ott-generated typing rules).
- Talk about the use and benefits of Copilot.