Destination calculus

A linear $\lambda-$calculus for pure, functional memory updates

ARNAUD SPIWACK, Modus Create, France
THOMAS BAGREL, LORIA/Inria, France and Modus Create, France

We present the destination calculus, a linear $\lambda-$calculus for pure, functional memory updates. We introduce the syntax, type system, and operational semantics of the destination calculus, and prove type safety formally in the Coq proof assistant.

We show how the principles of the destination calculus can form a theoretical ground for destination-passing style programming in functional languages. In particular, we detail how the present work can be applied to Linear Haskell to lift the main restriction of DPS programming in Haskell as developed in [1]. We illustrate this with a range of pseudo-Haskell examples.

ACM Reference Format:
Arnaud Spiwack and Thomas Bagrel. 2024. Destination calculus: A linear $\lambda-$calculus for pure, functional memory updates. In . ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 TERM AND VALUE SYNTAX

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

POPL'25, January 19 – 25, 2025, Denver, Colorado

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

hvar, h	::=			Hole or destination name ($\mathbb{N}$)
	|	$\mathsf{h}+\mathsf{h}'$	M	
	|	$\mathsf{h}[\mathsf{H}\stackrel{\pm}{=}\mathsf{h}']$	M	Shift by h' if $\mathsf{h} \in \mathsf{H}$
	|	$\mathit{max}(\mathsf{H})$	M	Maximum of a set of holes
hvars, H	::=			Set of hole names
	|	$\{\mathsf{h}_1, \,..\,, \mathsf{h}_k\}$		
	|	$\mathsf{H}_1 \cup \mathsf{H}_2$	M	Union of sets
	|	$\mathsf{H}\stackrel{\pm}{=}\mathsf{h}'$	M	Shift all names from H by h'.
	|	$\mathit{hvars}(\Gamma)$	M	Hole names of a context (requires `ctx`
	|	$\mathit{hvars}(C)$	M	Hole names of an evaluation context
term, *t*, *u*	::=			Term
	|	v		Value
	|	x		Variable
	|	$t \triangleright t'$		Application
	|	$t \,;\, u$		Pattern-match on unit
	|	$t \triangleright \mathtt{case}_{\mathsf{m}}\, \{\mathtt{Inl}\ \mathsf{x}_1 \mapsto u_1\,,\ \mathtt{Inr}\ \mathsf{x}_2 \mapsto u_2\}$		Pattern-match on sum
	|	$t \triangleright \mathtt{case}_{\mathsf{m}}\, (\mathsf{x}_1\,, \mathsf{x}_2) \mapsto u$		Pattern-match on product
	|	$t \triangleright \mathtt{case}_{\mathsf{m}}\, \mathsf{E}_{\mathsf{n}}\ \mathsf{x} \mapsto u$		Pattern-match on exponential
	|	$t \triangleright \mathtt{map}\ \mathsf{x} \mapsto t'$		Map over the right side of ampar t
	|	$\mathtt{to}_{\ltimes}\ u$		Wrap u into a trivial ampar
	|	$\mathtt{from}_{\ltimes}\ t$		Convert ampar with no dest remaining
	|	$t \triangleleft ()$		Fill destination with unit
	|	$t \triangleleft \mathtt{Inl}$		Fill destination with left variant
	|	$t \triangleleft \mathtt{Inr}$		Fill destination with right variant
	|	$t \triangleleft \mathsf{E}_{\mathsf{m}}$		Fill destination with exponential const

	|	$t \triangleleft (,)$		Fill destination with product constructor
	|	$t \triangleleft (\lambda x\ {}_{m}\mapsto\ u)$		Fill destination with function
	|	$t \triangleleft\!\bullet\ t'$		Fill destination with root of ampar t'
	|	$t[x := v]$	M	
$val,\ v$	::=			Term value
	|	$-h$		Hole
	|	$+h$		Destination
	|	$()$		Unit
	|	$\lambda^{v} x\ {}_{m}\mapsto\ u$		Lambda abstraction
	|	$\mathtt{Inl}\ v$		Left variant for sum
	|	$\mathtt{Inr}\ v$		Right variant for sum
	|	$E_{m}\ v$		Exponential
	|	$(v_1\ ,\ v_2)$		Product
	|	${}_{H}\langle v_2\ ⨟\ v_1\rangle$		Ampar
	|	$v[H \pm h']$	M	Shift hole names inside v by h' if they belong to H.

$ectx,\ c$	::=			Evaluation context component
	|	$\square \triangleright t'$		Application
	|	$v \triangleright \square$		Application
	|	$\square\ ;\ u$		Pattern-match on unit
	|	$\square \triangleright \mathtt{case}_{m}\ \{\mathtt{Inl}\ x_1\ \mapsto\ u_1\ ,\ \mathtt{Inr}\ x_2\ \mapsto\ u_2\}$		Pattern-match on sum
	|	$\square \triangleright \mathtt{case}_{m}\ (x_1\ ,\ x_2) \mapsto\ u$		Pattern-match on product
	|	$\square \triangleright \mathtt{case}_{m}\ E_{n}\ x\ \mapsto\ u$		Pattern-match on exponential
	|	$\square \triangleright \mathtt{map}\ x \mapsto\ t'$		Map over the right side of ampar
	|	$\mathtt{to}_{\ltimes}\ \square$		Wrap into a trivial ampar
	|	$\mathtt{from}_{\ltimes}\ \square$		Convert ampar with no dest remaining
	|	$\square \triangleleft ()$		Fill destination with unit
	|	$\square \triangleleft \mathtt{Inl}$		Fill destination with left variant
	|	$\square \triangleleft \mathtt{Inr}$		Fill destination with right variant
	|	$\square \triangleleft E_{m}$		Fill destination with exponential constr
	|	$\square \triangleleft (,)$		Fill destination with product constructo
	|	$\square \triangleleft (\lambda x\ {}_{m}\mapsto\ u)$		Fill destination with function
	|	$\square \triangleleft\!\bullet\ t'$		Fill destination with root of ampar
	|	$v \triangleleft\!\bullet\ \square$		Fill destination with root of ampar
	|	${}^{op}_{H}\langle v_2\ ⨟\ \square$		Open ampar. Only new addition to tern
$ectxs,\ C$	::=			Evaluation context stack
	|	$\square$		Represent the empty stack / "identity" e
	|	$C \circ c$		Push c on top of C
	|	$C[h :=_{H}\ v]$	M	Fill h in C with value v (that may conta

2 TYPE SYSTEM

type, T, U	::=			Type
	|	1		Unit
	|	$T_1 \oplus T_2$		Sum
	|	$T_1 \otimes T_2$		Product
	|	$!_m\, T$		Exponential
	|	$U \ltimes T$		Ampar type (consuming T yields U)
	|	$T\ {}_m\!\!\to U$		Function
	|	$\lfloor T \rfloor^m$		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
	|	ω		Non-linear. Absorbing for the product
	|	$p_1 . \ldots . p_k$	M	Semiring product
age, a	::=			Age (second component of modality)
	|	ν		Born now. Neutral element of the product
	|	$\uparrow$		One scope older
	|	∞		Infinitely old / static. Absorbing for the product
	|	$a_1 \cdot \ldots \cdot a_k$	M	Semiring product
ctx, Γ, Δ, Π	::=			Typing context
	|	$x :_m T$		
	|	$+h :_m \lfloor T \rfloor^n$		
	|	$-h : T^n$		
	|	$m \cdot \Gamma$	M	Multiply each binding by m
	|	$\Gamma_1 + \Gamma_2$	M	Sum contexts Γ_1 and Γ_2. Duplicate keys with incompatible values
	|	$\Gamma_1,\ \Gamma_2$	M	Disjoint sum/union of contexts Γ_1 and Γ_2.
	|	$-\Gamma$	M	Transforms dest bindings into a hole bindings (requires ctx_Dest
	|	$-^{-1}\Gamma$	M	Transforms hole bindings into dest bindings with left mode 1ν (re
	|	$\Gamma[H \pm h']$	M	Shift hole/dest names by h' if they belong to H

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

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

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

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

$$\textsc{TyR-val-F}\quad \frac{\Delta + x :_{\mathsf{m}} \mathsf{T} \vdash u : \mathsf{U}}{\Delta \Vdash \lambda^{\mathsf{v}} x\, {}_{\mathsf{m}}\!\mapsto u : \mathsf{T}\, {}_{\mathsf{m}}\!\!\to \mathsf{U}}$$

$$\textsc{TyR-val-L}\quad \frac{\Gamma \Vdash v_1 : \mathsf{T}_1}{\Gamma \Vdash \mathtt{Inl}\ v_1 : \mathsf{T}_1 \oplus \mathsf{T}_2}$$

$$\textsc{TyR-val-R}\quad \frac{\Gamma \Vdash v_2 : \mathsf{T}_2}{\Gamma \Vdash \mathtt{Inr}\ v_2 : \mathsf{T}_1 \oplus \mathsf{T}_2}$$

$$\textsc{TyR-val-P}\quad \frac{\begin{array}{c}\Gamma_1 \Vdash v_1 : \mathsf{T}_1 \\ \Gamma_2 \Vdash v_2 : \mathsf{T}_2\end{array}}{\Gamma_1 + \Gamma_2 \Vdash (v_1\, ,\, v_2) : \mathsf{T}_1 \otimes \mathsf{T}_2}$$

$$\textsc{TyR-val-E}\quad \frac{\Gamma \Vdash v' : \mathsf{T}}{\mathsf{n} \cdot \Gamma \Vdash \mathsf{E}_{\mathsf{n}}\ v' : !_{\mathsf{n}} \mathsf{T}}$$

$$\textsc{TyR-val-A}\quad \frac{\begin{array}{c}\mathtt{LinOnly}\ \Delta_3 \\ \mathtt{FinAgeOnly}\ \Delta_3 \\ 1\!\uparrow \cdot \Delta_1,\ \Delta_3 \Vdash v_1 : \mathsf{T} \\ \Delta_2,\ (-\Delta_3) \Vdash v_2 : \mathsf{U}\end{array}}{\Delta_1,\ \Delta_2 \Vdash {}_{\mathit{hvars}(-\Delta_3)}\langle v_2 \,;\, v_1 \rangle : \mathsf{U} \ltimes \mathsf{T}}$$

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

$$\textsc{Ty-term-Val}\quad \frac{\begin{array}{c}\mathtt{DisposableOnly}\ \Pi \\ \Delta \Vdash v : \mathsf{T}\end{array}}{\Pi,\ \Delta \vdash v : \mathsf{T}}$$

$$\textsc{Ty-term-Var}\quad \frac{\begin{array}{c}\mathtt{DisposableOnly}\ \Pi \\ 1\nu <: \mathsf{m}\end{array}}{\Pi,\ x :_{\mathsf{m}} \mathsf{T} \vdash x : \mathsf{T}}$$

$$\textsc{Ty-term-App}\quad \frac{\begin{array}{c}\Pi_1 \vdash t : \mathsf{T} \\ \Pi_2 \vdash t' : \mathsf{T}\, {}_{\mathsf{m}}\!\!\to \mathsf{U}\end{array}}{\mathsf{m} \cdot \Pi_1 + \Pi_2 \vdash t \rhd t' : \mathsf{U}}$$

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

$$\textsc{Ty-term-PatS}\quad \frac{\begin{array}{c}\Pi_1 \vdash t : \mathsf{T}_1 \oplus \mathsf{T}_2 \\ \Pi_2,\ x_1 :_{\mathsf{m}} \mathsf{T}_1 \vdash u_1 : \mathsf{U} \\ \Pi_2,\ x_2 :_{\mathsf{m}} \mathsf{T}_2 \vdash u_2 : \mathsf{U}\end{array}}{\mathsf{m} \cdot \Pi_1 + \Pi_2 \vdash t \rhd \mathtt{case}_{\mathsf{m}}\ \{\mathtt{Inl}\ x_1 \mapsto u_1\, ,\ \mathtt{Inr}\ x_2 \mapsto u_2\} : \mathsf{U}}$$

$$\textsc{Ty-term-PatP}\quad \frac{\begin{array}{c}\Pi_1 \vdash t : \mathsf{T}_1 \otimes \mathsf{T}_2 \\ \Pi_2,\ x_1 :_{\mathsf{m}} \mathsf{T}_1,\ x_2 :_{\mathsf{m}} \mathsf{T}_2 \vdash u : \mathsf{U}\end{array}}{\mathsf{m} \cdot \Pi_1 + \Pi_2 \vdash t \rhd \mathtt{case}_{\mathsf{m}}\ (x_1\, ,\, x_2) \mapsto u : \mathsf{U}}$$

$$\textsc{Ty-term-PatE}\quad \frac{\begin{array}{c}\Pi_1 \vdash t : !_{\mathsf{n}} \mathsf{T} \\ \Pi_2,\ x :_{\mathsf{m} \cdot \mathsf{n}} \mathsf{T} \vdash u : \mathsf{U}\end{array}}{\mathsf{m} \cdot \Pi_1 + \Pi_2 \vdash t \rhd \mathtt{case}_{\mathsf{m}}\ \mathsf{E}_{\mathsf{n}}\ x \mapsto u : \mathsf{U}}$$

$$\textsc{Ty-term-Map}\quad \frac{\begin{array}{c}\Pi_1 \vdash t : \mathsf{U} \ltimes \mathsf{T} \\ 1\!\uparrow \cdot \Pi_2,\ x :_{1\nu} \mathsf{T} \vdash t' : \mathsf{T}'\end{array}}{\Pi_1 + \Pi_2 \vdash t \rhd \mathtt{map}\ x \mapsto t' : \mathsf{U} \ltimes \mathsf{T}'}$$

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

$$\textsc{Ty-term-FromA}\quad \frac{\Pi \vdash t : \mathsf{U} \ltimes (!_{1\infty}\, \mathsf{T})}{\Pi \vdash \mathtt{from}_{\ltimes}\ t : \mathsf{U} \otimes (!_{1\infty}\, \mathsf{T})}$$

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

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

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

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

$$\textsc{Ty-term-FillE}\quad \frac{\Pi \vdash t : \lfloor !_{\mathsf{n}'}\, \mathsf{T} \rfloor^{\mathsf{n}}}{\Pi \vdash t \triangleleft \mathsf{E}_{\mathsf{n}'} : \lfloor \mathsf{T} \rfloor^{\mathsf{n}' \cdot \mathsf{n}}}$$

$$\textsc{Ty-term-FillF}\quad \frac{\begin{array}{c}\Pi_1 \vdash t : \lfloor \mathsf{T}\, {}_{\mathsf{m}}\!\!\to \mathsf{U} \rfloor^{\mathsf{n}} \\ \Pi_2,\ x :_{\mathsf{m}} \mathsf{T} \vdash u : \mathsf{U}\end{array}}{\Pi_1 + (1\!\uparrow \cdot \mathsf{n}) \cdot \Pi_2 \vdash t \triangleleft (\lambda x\, {}_{\mathsf{m}}\!\mapsto u) : \mathsf{1}}$$

$$\textsc{Ty-term-FillC}\quad \frac{\begin{array}{c}\Pi_1 \vdash t : \lfloor \mathsf{U} \rfloor^{\mathsf{n}} \\ \Pi_2 \vdash t' : \mathsf{U} \ltimes \mathsf{T}\end{array}}{\Pi_1 + (1\!\uparrow \cdot \mathsf{n}) \cdot \Pi_2 \vdash t \triangleleft\!\bullet\, t' : \mathsf{T}}$$

$\boxed{\Delta \dashv C : \mathsf{T} \rightarrowtail \mathsf{U}_0}$ *(Typing of evaluation contexts)*

$$\textsc{Ty-ectxs-Id}\quad \frac{}{\dashv \square : \mathsf{U}_0 \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-AppFoc1}\quad \frac{\mathsf{m}\cdot\Delta_1,\ \Delta_2 \dashv C : \mathsf{U} \rightarrowtail \mathsf{U}_0 \qquad \Delta_2 \vdash t' : \mathsf{T}\ {}_{\mathsf{m}}{\rightarrow}\ \mathsf{U}}{\Delta_1 \dashv C \circ (\square \rhd t') : \mathsf{T} \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-AppFoc2}\quad \frac{\mathsf{m}\cdot\Delta_1,\ \Delta_2 \dashv C : \mathsf{U} \rightarrowtail \mathsf{U}_0 \qquad \Delta_1 \vdash v : \mathsf{T}}{\Delta_2 \dashv C \circ (v \rhd \square) : (\mathsf{T}\ {}_{\mathsf{m}}{\rightarrow}\ \mathsf{U}) \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-PatUFoc}\quad \frac{\Delta_1,\ \Delta_2 \dashv C : \mathsf{U} \rightarrowtail \mathsf{U}_0 \qquad \Delta_2 \vdash u : \mathsf{U}}{\Delta_1 \dashv C \circ (\square\, ;\, u) : \mathsf{1} \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-PatSFoc}\quad \frac{\mathsf{m}\cdot\Delta_1,\ \Delta_2 \dashv C : \mathsf{U} \rightarrowtail \mathsf{U}_0 \qquad \Delta_2,\ x_1 :_{\mathsf{m}} \mathsf{T}_1 \vdash u_1 : \mathsf{U} \qquad \Delta_2,\ x_2 :_{\mathsf{m}} \mathsf{T}_2 \vdash u_2 : \mathsf{U}}{\Delta_1 \dashv C \circ (\square \rhd \mathtt{case}_{\mathsf{m}}\ \{\mathtt{Inl}\ x_1 \mapsto u_1\,,\ \mathtt{Inr}\ x_2 \mapsto u_2\}) : (\mathsf{T}_1 \oplus \mathsf{T}_2) \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-PatPFoc}\quad \frac{\mathsf{m}\cdot\Delta_1,\ \Delta_2 \dashv C : \mathsf{U} \rightarrowtail \mathsf{U}_0 \qquad \Delta_2,\ x_1 :_{\mathsf{m}} \mathsf{T}_1,\ x_2 :_{\mathsf{m}} \mathsf{T}_2 \vdash u : \mathsf{U}}{\Delta_1 \dashv C \circ (\square \rhd \mathtt{case}_{\mathsf{m}}\ (x_1\,,\, x_2) \mapsto u) : (\mathsf{T}_1 \otimes \mathsf{T}_2) \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-PatEFoc}\quad \frac{\mathsf{m}\cdot\Delta_1,\ \Delta_2 \dashv C : \mathsf{U} \rightarrowtail \mathsf{U}_0 \qquad \Delta_2,\ x :_{\mathsf{m}\cdot\mathsf{m}'} \mathsf{T} \vdash u : \mathsf{U}}{\Delta_1 \dashv C \circ (\square \rhd \mathtt{case}_{\mathsf{m}}\ \mathsf{E}_{\mathsf{m}'}\ x \mapsto u) : !_{\mathsf{m}'}\ \mathsf{T} \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-MapFoc}\quad \frac{\Delta_1,\ \Delta_2 \dashv C : \mathsf{U} \ltimes \mathsf{T}' \rightarrowtail \mathsf{U}_0 \qquad \mathsf{1}{\uparrow}\cdot\Delta_2,\ x :_{\mathsf{1}\nu} \mathsf{T} \vdash t' : \mathsf{T}'}{\Delta_1 \dashv C \circ (\square \rhd \mathtt{map}\ x \mapsto t') : (\mathsf{U} \ltimes \mathsf{T}) \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-ToAFoc}\quad \frac{\Delta \dashv C : (\mathsf{U} \ltimes \mathsf{1}) \rightarrowtail \mathsf{U}_0}{\Delta \dashv C \circ (\mathtt{to}_{\ltimes}\ \square) : \mathsf{U} \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-FromAFoc}\quad \frac{\Delta \dashv C : (\mathsf{U} \otimes (!_{\mathsf{1}\infty}\ \mathsf{T})) \rightarrowtail \mathsf{U}_0}{\Delta \dashv C \circ (\mathtt{from}_{\ltimes}\ \square) : (\mathsf{U} \ltimes (!_{\mathsf{1}\infty}\ \mathsf{T})) \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-FillUFoc}\quad \frac{\Delta \dashv C : \mathsf{1} \rightarrowtail \mathsf{U}_0}{\Delta \dashv C \circ (\square \blacktriangleleft ()) : \lfloor \mathsf{1} \rfloor^{\mathsf{n}} \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-FillLFoc}\quad \frac{\Delta \dashv C : \lfloor \mathsf{T}_1 \rfloor^{\mathsf{n}} \rightarrowtail \mathsf{U}_0}{\Delta \dashv C \circ (\square \blacktriangleleft \mathtt{Inl}) : \lfloor \mathsf{T}_1 \oplus \mathsf{T}_2 \rfloor^{\mathsf{n}} \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-FillRFoc}\quad \frac{\Delta \dashv C : \lfloor \mathsf{T}_2 \rfloor^{\mathsf{n}} \rightarrowtail \mathsf{U}_0}{\Delta \dashv C \circ (\square \blacktriangleleft \mathtt{Inr}) : \lfloor \mathsf{T}_1 \oplus \mathsf{T}_2 \rfloor^{\mathsf{n}} \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-FillPFoc}\quad \frac{\Delta \dashv C : (\lfloor \mathsf{T}_1 \rfloor^{\mathsf{n}} \otimes \lfloor \mathsf{T}_2 \rfloor^{\mathsf{n}}) \rightarrowtail \mathsf{U}_0}{\Delta \dashv C \circ (\square \blacktriangleleft (,)) : \lfloor \mathsf{T}_1 \otimes \mathsf{T}_2 \rfloor^{\mathsf{n}} \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-FillEFoc}\quad \frac{\Delta \dashv C : \lfloor \mathsf{T} \rfloor^{\mathsf{m}\cdot\mathsf{n}} \rightarrowtail \mathsf{U}_0}{\Delta \dashv C \circ (\square \blacktriangleleft \mathsf{E}_{\mathsf{m}}) : \lfloor !_{\mathsf{m}}\ \mathsf{T} \rfloor^{\mathsf{n}} \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-FillFFoc}\quad \frac{\Delta_1,\ (\mathsf{1}{\uparrow}\cdot\mathsf{n})\cdot\Delta_2 \dashv C : \mathsf{1} \rightarrowtail \mathsf{U}_0 \qquad \Delta_2,\ x :_{\mathsf{m}} \mathsf{T} \vdash u : \mathsf{U}}{\Delta_1 \dashv C \circ (\square \blacktriangleleft (\lambda x\ {}_{\mathsf{m}}{\mapsto}\ u)) : \lfloor \mathsf{T}\ {}_{\mathsf{m}}{\rightarrow}\ \mathsf{U} \rfloor^{\mathsf{n}} \rightarrowtail \mathsf{U}_0}$$

$$\textsc{Ty-ectxs-FillCFoc1}\quad \frac{\Delta_1,\ (1\uparrow\cdot n)\cdot\Delta_2 \dashv C : T \rightarrowtail U_0 \qquad \Delta_2 \vdash t' : U \ltimes T}{\Delta_1 \dashv C \circ (\square \triangleleft\!\bullet\, t') : \lfloor U \rfloor^{n} \rightarrowtail U_0}$$

$$\textsc{Ty-ectxs-FillCFoc2}\quad \frac{\Delta_1,\ (1\uparrow\cdot n)\cdot\Delta_2 \dashv C : T \rightarrowtail U_0 \qquad \Delta_1 \vdash v : \lfloor U \rfloor^{n}}{\Delta_2 \dashv C \circ (v \triangleleft\!\bullet\, \square) : U \ltimes T \rightarrowtail U_0}$$

$$\textsc{Ty-ectxs-AOpenFoc}\quad \frac{hvars(C)\ \#\#\ hvars(-\Delta_3) \qquad \mathtt{LinOnly}\ \Delta_3 \qquad \mathtt{FinAgeOnly}\ \Delta_3 \qquad \Delta_1,\ \Delta_2 \dashv C : (U \ltimes T') \rightarrowtail U_0 \qquad \Delta_2,\ -\Delta_3 \Vdash v_2 : U}{1\uparrow\cdot\Delta_1,\ \Delta_3 \dashv C \circ ({}^{\mathrm{op}}_{hvars(-\Delta_3)}\langle v_2 \,;\, \square) : T' \rightarrowtail U_0}$$

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

$$\textsc{Ty-eterm-ClosedEterm}\quad \frac{\Delta \dashv C : T \rightarrowtail U_0 \qquad \Delta \vdash t : T}{\vdash C[t] : U_0}$$

3 SMALL-STEP SEMANTICS

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

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

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

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

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

$$\textsc{Sem-eterm-AppRed}\quad \frac{}{C[v \rhd (\lambda^{\mathsf{v}} \mathsf{x}\,_{\mathsf{m}} \mapsto\ u)] \longrightarrow C[u[\mathsf{x} \coloneqq v]]}$$

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

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

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

$$\textsc{Sem-eterm-PatSFoc}\quad \frac{\texttt{NotVal}\ \ t}{C[t \rhd \texttt{case}_{\mathsf{m}}\, \{\texttt{Inl}\ \mathsf{x}_1 \mapsto u_1\,,\ \texttt{Inr}\ \mathsf{x}_2 \mapsto u_2\}] \longrightarrow (C \circ (\square \rhd \texttt{case}_{\mathsf{m}}\, \{\texttt{Inl}\ \mathsf{x}_1 \mapsto u_1\,,\ \texttt{Inr}\ \mathsf{x}_2 \mapsto u_2\}))[t]}$$

$$\textsc{Sem-eterm-PatSUnfoc}\quad \frac{}{(C \circ (\square \rhd \texttt{case}_{\mathsf{m}}\, \{\texttt{Inl}\ \mathsf{x}_1 \mapsto u_1\,,\ \texttt{Inr}\ \mathsf{x}_2 \mapsto u_2\}))[v] \longrightarrow C[v \rhd \texttt{case}_{\mathsf{m}}\, \{\texttt{Inl}\ \mathsf{x}_1 \mapsto u_1\,,\ \texttt{Inr}\ \mathsf{x}_2 \mapsto u_2\}]}$$

$$\textsc{Sem-eterm-PatLRed}\quad \frac{}{C[(\texttt{Inl}\ v_1) \rhd \texttt{case}_{\mathsf{m}}\, \{\texttt{Inl}\ \mathsf{x}_1 \mapsto u_1\,,\ \texttt{Inr}\ \mathsf{x}_2 \mapsto u_2\}] \longrightarrow C[u_1[\mathsf{x}_1 \coloneqq v_1]]}$$

$$\textsc{Sem-eterm-PatRRed}\quad \frac{}{C[(\texttt{Inr}\ v_2) \rhd \texttt{case}_{\mathsf{m}}\, \{\texttt{Inl}\ \mathsf{x}_1 \mapsto u_1\,,\ \texttt{Inr}\ \mathsf{x}_2 \mapsto u_2\}] \longrightarrow C[u_2[\mathsf{x}_2 \coloneqq v_2]]}$$

$$\textsc{Sem-eterm-PatPFoc}\quad \frac{\texttt{NotVal}\ \ t}{C[t \rhd \texttt{case}_{\mathsf{m}}\, (\mathsf{x}_1\,,\mathsf{x}_2) \mapsto u] \longrightarrow (C \circ (\square \rhd \texttt{case}_{\mathsf{m}}\, (\mathsf{x}_1\,,\mathsf{x}_2) \mapsto u))[t]}$$

$$\textsc{Sem-eterm-PatPUnfoc}\quad \frac{}{(C \circ (\square \rhd \texttt{case}_{\mathsf{m}}\, (\mathsf{x}_1\,,\mathsf{x}_2) \mapsto u))[v] \longrightarrow C[v \rhd \texttt{case}_{\mathsf{m}}\, (\mathsf{x}_1\,,\mathsf{x}_2) \mapsto u]}$$

$$\textsc{Sem-eterm-PatPRed}\quad \frac{}{C[(v_1\,,v_2) \rhd \texttt{case}_{\mathsf{m}}\, (\mathsf{x}_1\,,\mathsf{x}_2) \mapsto u] \longrightarrow C[u[\mathsf{x}_1 \coloneqq v_1][\mathsf{x}_2 \coloneqq v_2]]}$$

$$\textsc{Sem-eterm-PatEFoc}\quad \frac{\texttt{NotVal}\ \ t}{C[t \rhd \texttt{case}_{\mathsf{m}}\, \mathsf{E}_{\mathsf{n}}\ \mathsf{x} \mapsto u] \longrightarrow (C \circ (\square \rhd \texttt{case}_{\mathsf{m}}\, \mathsf{E}_{\mathsf{n}}\ \mathsf{x} \mapsto u))[t]}$$

$$\textsc{Sem-eterm-PatEUnfoc}\quad \frac{}{(C \circ (\square \triangleright \mathtt{case}_{\mathsf{m}}\ \mathsf{E}_{\mathsf{n}}\ \mathsf{x} \mapsto u))[v] \longrightarrow C[v \triangleright \mathtt{case}_{\mathsf{m}}\ \mathsf{E}_{\mathsf{n}}\ \mathsf{x} \mapsto u]}$$

$$\textsc{Sem-eterm-PatERed}\quad \frac{}{C[\mathsf{E}_{\mathsf{n}}\ v' \triangleright \mathtt{case}_{\mathsf{m}}\ \mathsf{E}_{\mathsf{n}}\ \mathsf{x} \mapsto u] \longrightarrow C[u[\mathsf{x} \coloneqq v']]}$$

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

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

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

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

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

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

$$\textsc{Sem-eterm-ToARed}\quad \frac{}{C[\mathtt{to}_{\ltimes}\ v_2] \longrightarrow C[{}_{\{\}}\langle v_2 \mathbin{;} ()\rangle]}$$

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

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

$$\textsc{Sem-eterm-FromARed}\quad \frac{}{C[\mathtt{from}_{\ltimes}\ {}_{\{\}}\langle v_2 \mathbin{;} \mathsf{E}_{1\infty}\ v_1\rangle] \longrightarrow C[(v_2\ , \mathsf{E}_{1\infty}\ v_1)]}$$

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

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

$$\textsc{Sem-eterm-FillURed}\quad \frac{}{C[+\mathsf{h} \triangleleft ()] \longrightarrow C[\mathsf{h} \coloneqq_{\{\}}\ ()][()]}$$

$$\textsc{Sem-eterm-FillLFoc}\quad \frac{\mathtt{NotVal}\ \ t}{C[t \triangleleft \mathtt{Inl}] \longrightarrow (C \circ (\square \triangleleft \mathtt{Inl}))[t]}$$

$$\textsc{Sem-eterm-FillLUnfoc}\quad \frac{}{(C \circ (\square \triangleleft \mathtt{Inl}))[v] \longrightarrow C[v \triangleleft \mathtt{Inl}]}$$

$$\textsc{Sem-eterm-FillLRed}\quad \frac{\mathsf{h}' \ = \ \mathit{max}(\mathit{hvars}(C) \cup \{\mathsf{h}\})+1}{C[+\mathsf{h} \triangleleft \mathtt{Inl}] \longrightarrow C[\mathsf{h} \coloneqq_{\{\mathsf{h}'+1\}}\ \mathtt{Inl}\ -(\mathsf{h}'+1)][+(\mathsf{h}'+1)]}$$

$$\textsc{Sem-eterm-FillRFoc}\quad \frac{\mathtt{NotVal}\ \ t}{C[t \triangleleft \mathtt{Inr}] \longrightarrow (C \circ (\square \triangleleft \mathtt{Inr}))[t]}$$

$$\textsc{Sem-eterm-FillRUnfoc}\quad \frac{}{(C \circ (\square \triangleleft \mathtt{Inr}))[v] \longrightarrow C[v \triangleleft \mathtt{Inr}]}$$

$$\textsc{Sem-eterm-FillRRed}\quad \frac{\mathsf{h}' \ = \ \mathit{max}(\mathit{hvars}(C) \cup \{\mathsf{h}\})+1}{C[+\mathsf{h} \triangleleft \mathtt{Inr}] \longrightarrow C[\mathsf{h} \coloneqq_{\{\mathsf{h}'+1\}}\ \mathtt{Inr}\ -(\mathsf{h}'+1)][+(\mathsf{h}'+1)]}$$

$$\frac{\text{NotVal}\ t}{C[t \triangleleft \mathsf{E_m}] \longrightarrow (C \circ (\square \triangleleft \mathsf{E_m}))[t]}\ \textsc{Sem-eterm-FillEFoc}$$

$$\frac{}{(C \circ (\square \triangleleft \mathsf{E_m}))[v] \longrightarrow C[v \triangleleft \mathsf{E_m}]}\ \textsc{Sem-eterm-FillEUnfoc}$$

$$\frac{\mathsf{h}' = \mathit{max}(\mathit{hvars}(C) \cup \{\mathsf{h}\}) + 1}{C[+\mathsf{h} \triangleleft \mathsf{E_m}] \longrightarrow C[\mathsf{h} :=_{\{\mathsf{h}'+1\}} \mathsf{E_m} - (\mathsf{h}'+1)][+(\mathsf{h}'+1)]}\ \textsc{Sem-eterm-FillERed}$$

$$\frac{\text{NotVal}\ t}{C[t \triangleleft (,)] \longrightarrow (C \circ (\square \triangleleft (,)))[t]}\ \textsc{Sem-eterm-FillPFoc}$$

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

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

$$\frac{\text{NotVal}\ t}{C[t \triangleleft (\lambda \mathsf{x}\ {}_{\mathsf{m}}\mapsto\ u)] \longrightarrow (C \circ (\square \triangleleft (\lambda \mathsf{x}\ {}_{\mathsf{m}}\mapsto\ u)))[t]}\ \textsc{Sem-eterm-FillFFoc}$$

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

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

$$\frac{\text{NotVal}\ t}{C[t \triangleleft\!\bullet\ t'] \longrightarrow (C \circ (\square \triangleleft\!\bullet\ t'))[t]}\ \textsc{Sem-eterm-FillCFoc1}$$

$$\frac{}{(C \circ (\square \triangleleft\!\bullet\ t'))[v] \longrightarrow C[v \triangleleft\!\bullet\ t']}\ \textsc{Sem-eterm-FillCUnfoc1}$$

$$\frac{\text{NotVal}\ t'}{C[v \triangleleft\!\bullet\ t'] \longrightarrow (C \circ (v \triangleleft\!\bullet \square))[t']}\ \textsc{Sem-eterm-FillCFoc2}$$

$$\frac{}{(C \circ (v \triangleleft\!\bullet \square))[v'] \longrightarrow C[v \triangleleft\!\bullet\ v']}\ \textsc{Sem-eterm-FillCUnfoc2}$$

$$\frac{\mathsf{h}' = \mathit{max}(\mathit{hvars}(C) \cup \{\mathsf{h}\}) + 1}{C[+\mathsf{h} \triangleleft\!\bullet_{\mathsf{H}} \langle v_2 \,,\, v_1 \rangle] \longrightarrow C[\mathsf{h} :=_{(\mathsf{H} \pm \mathsf{h}')} v_2[\mathsf{H} \pm \mathsf{h}']][v_1[\mathsf{H} \pm \mathsf{h}']]}\ \textsc{Sem-eterm-FillCRed}$$

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.

REFERENCES

[1] Thomas Bagrel. 2024. Destination-passing style programming: a Haskell implementation. https://inria.hal.science/hal-04406360