Modalities and Erasure in a Dependently Typed Language

Oskar Eriksson, Andreas Abel

Chalmers and Gothenburg University

28th Conf. on Types for Proofs and Programs
TYPES 2022, Nantes, France
21 June 2022

Introduction

- Petricek, Orchard, Mycroft, ICFP 2014: Coeffects
- McBride, 2016: *I got plenty of nuttin'*
- Atkey, LiCS 2018: Quantitative Type Theory
- Wood, Atkey, 2020: A Linear Algebra Approach to Linear Metatheory
- A. TYPES 2018: Resourceful Dependent Types
- Oskar Eriksson 2021-22: Agda formalization

Quantitative analysis

- One reference to a variable = one use
- Correct reference count under call-by-name

$$(\lambda x \lambda u.\ x + x)\ y\ z$$

var	name	need	value
y	2	1	1
z	0	0	1

- Usage judgement $\boxed{\gamma \rhd t}$

$$y : 2,\ z : 0 \rhd (\lambda x \lambda u.\ x + x)\ y\ z$$

Aggregation: sum

$$\frac{\gamma_1 \rhd t_1 \qquad \gamma_2 \rhd t_2}{\gamma_1 + \gamma_2 \rhd (t_1, t_2)}$$

$$(\gamma_1 + \gamma_2)(x) = \gamma_1(x) + \gamma_2(x)$$

Choice?

$$
\begin{array}{lcl}
\mathsf{bool}\ (t\ f : A) & : & \mathsf{Bool} \to A \\
\mathsf{bool}\ t\ f\ \mathsf{true} & = & t \\
\mathsf{bool}\ t\ f\ \mathsf{false} & = & f
\end{array}
$$

$$
\frac{\gamma_1 \rhd t \qquad \gamma_2 \rhd f}{? \rhd \mathsf{bool}\ t\ f}
$$

Choice: meet

$$\frac{\gamma_1 \rhd t \qquad \gamma_2 \rhd f}{\gamma_1 \wedge \gamma_2 \rhd \mathsf{bool}\ t\ f}$$

$$\begin{aligned}
\gamma(x) &\subseteq \mathbb{N} \\
(\gamma_1 \wedge \gamma_2)(x) &= \gamma_1(x) \cup \gamma_2(x) \\
(\gamma_1 + \gamma_2)(x) &= \{m + n \mid m \in \gamma_1(x), n \in \gamma_2(x)\}
\end{aligned}$$

$$\begin{tikzcd}
\{0\} \arrow[dr, dash] & & \{1\} \arrow[dl, dash] \arrow[dr, dash] & & \mathbb{N} \setminus \{0,1\} \arrow[dl, dash] \\
& \{0,1\} \arrow[dr, dash] & & \mathbb{N} \setminus \{0\} \arrow[dl, dash] & \\
& & \mathbb{N} & &
\end{tikzcd}$$

Subsumption: precision loss

$$\frac{\delta \rhd t}{\gamma \rhd t}\ \gamma \leq \delta \qquad \text{e.g. } \frac{x{:}\{1\} \rhd x}{x{:}\{0,1\} \rhd x}$$

Application: scaling

$$\frac{\gamma, x{:}p \rhd t}{\gamma \rhd \lambda^p x.\ t} \qquad \frac{\gamma \rhd t \qquad \delta \rhd u}{\gamma + p\delta \rhd t\ {}^p u}$$

$$\frac{\rhd (\lambda^2 x \lambda^0 u.\ x + x) \qquad y : 1 \rhd y \qquad z : 1 \rhd z}{y : 2,\ z : 0 \rhd (\lambda^2 x \lambda^0 u.\ x + x)\ {}^2 y\ {}^0 z}$$

Modality structure $\mathbb{M}$

- Partially ordered semiring $(M, +, \cdot, \wedge, 0, 1)$
- $+$ and $\cdot$ are monotone (distribute over $\wedge$)
- $+$ and $\wedge$ are commutative
- $0, 1$ for variable usage

$$x{:}0, y{:}1, z{:}0 \rhd y$$

Erasure

- Which function arguments can be safely erased?

$$\begin{array}{ccccl} 0 & = & \{0\} & & \text{unused, erase} \\ | & & & & \\ \omega & = & \mathbb{N} & & \text{used, keep} \end{array}$$

- $p + q = p \wedge q$
- $1 = \omega$

Security / privacy

- Which information is kept confidential?

$$\begin{array}{cccl} \mathsf{H} & = & \{0\} & \text{private, confidential} \\ | & & & \\ \mathsf{L} & = & \mathbb{N} & \text{public, observable} \end{array}$$

- Same as erasure!

$$\frac{\mathit{user}{:}\mathsf{L} \rhd \mathit{user} \qquad \mathit{pwd}{:}\mathsf{L} \rhd \mathit{pwd}}{\mathit{user}{:}\mathsf{L},\ \mathit{pwd}{:}\mathsf{H} \rhd \text{authenticate}\ {}^{\mathsf{L}}\mathit{user}\ {}^{\mathsf{H}}\mathit{pwd}}$$

$\lambda_{\mathbb{M}}^{\Sigma\Pi\mathsf{U}\mathbb{N}}$

- De Bruijn syntax:

$$
\begin{array}{lcl}
F, G, t, u & ::= & \mathsf{U} \mid \mathbb{N} \mid \top \mid \bot \mid \Pi_p^q\, F\, G \mid \Sigma_k^q\, F\, G \\
& \mid & x_i \mid \lambda^p\, t \mid t\,{}^p u \\
& \mid & (t, u) \mid \mathsf{fst}\, t \mid \mathsf{snd}\, t \mid \mathsf{prodrec}_p\, A\, t\, u \\
& \mid & \mathsf{zero} \mid \mathsf{suc}\, t \mid \mathsf{natrec}_p^r\, A\, z\, s\, n \\
& \mid & \star \mid \mathsf{emptyrec}_p\, A\, t \\
k & ::= & \times \mid \otimes
\end{array}
$$

- Typing relations:

$$
\Gamma \vdash t : A \qquad \gamma \triangleright t
$$

Usage relation for types

$$\frac{}{\mathbf{0} \rhd \mathsf{U}} \qquad \frac{}{\mathbf{0} \rhd \mathbb{N}} \qquad \frac{}{\mathbf{0} \rhd \top} \qquad \frac{}{\mathbf{0} \rhd \bot}$$

$$\frac{\gamma \rhd F \qquad \delta, q \rhd G}{\gamma + \delta \rhd \Pi_p^q\, F\, G} \qquad \frac{\gamma \rhd F \qquad \delta, q \rhd G}{\gamma + \delta \rhd \Sigma_k^q\, F\, G}$$

Typing functions

$$\frac{\Gamma, F \vdash t : G}{\Gamma \vdash \lambda^{p}\, t : \Pi_{p}^{q}\, F\, G}$$

$$\frac{\Gamma \vdash t : \Pi_{p}^{q}\, F\, G \qquad \Gamma \vdash u : F}{\Gamma \vdash t\, {}^{p} u : G[u]}$$

Typing pairs

- Introduction

$$\frac{\Gamma \vdash t_1 : F \qquad \Gamma \vdash t_2 : G[t_1]}{\Gamma \vdash (t_1, t_2) : \Sigma^q_k\, F\, G}$$

- Projections ($\times$)

$$\frac{\Gamma \vdash t : \Sigma^q_\times\, F\, G}{\Gamma \vdash \mathrm{fst}\, t : F} \qquad \frac{\Gamma \vdash t : \Sigma^q_\times\, F\, G}{\Gamma \vdash \mathrm{snd}\, t : G[\mathrm{fst}\, t]}$$

- Split ($\otimes$)

$$\frac{\Gamma \vdash t : \Sigma^q_k\, F\, G \qquad \Gamma, F, G \vdash u : A}{\Gamma \vdash \mathrm{prodrec}_p\, A\, t\, u : A}$$

Usage relation for Σ-elimination

$$\frac{\mathbf{0} \rhd t}{\mathbf{0} \rhd \mathsf{fst}\ t} \qquad \frac{\mathbf{0} \rhd t}{\mathbf{0} \rhd \mathsf{snd}\ t}$$

$$\frac{\gamma \rhd t \quad \delta, p, p \rhd u}{p\gamma + \delta \rhd \mathsf{prodrec}_p\ A\ t\ u}$$

Subject reduction

If $\gamma \triangleright t$ and $t \longrightarrow u$ then $\delta \triangleright u$ for some $\delta \geq \gamma$.

Subject reduction (example)

$$\dfrac{\dfrac{\gamma_1 \rhd t_1 \quad \gamma_2 \rhd t_2}{\gamma_1 + \gamma_2 \rhd (t_1, t_2)} \quad \delta, q, q \rhd u}{q(\gamma_1 + \gamma_2) + \delta \ \rhd\ \mathrm{prodrec}_q\, A\,(t_1, t_2)\, u}$$

$$\downarrow$$

$$\delta + q\gamma_1 + q\gamma_2 \ \rhd\ u[t_1, t_2]$$

Recursion

$$\mathsf{fix}\ s \longrightarrow s[\mathsf{fix}\ s] \longrightarrow s[s[\mathsf{fix}\ s]] \longrightarrow \dots$$

$$\frac{\sigma, r \triangleright s}{\phi \triangleright \mathsf{fix}\ s}$$

$$\phi \leq \sigma + r\phi \leq \sigma + r(\sigma + r\phi) \leq \cdots \leq \sum_{i \in \mathbb{N}} r^i \sigma = r^* \sigma$$

Recursion over $\mathbb{N}$

$$\frac{\nu \triangleright n \quad \zeta \triangleright z \quad \sigma, p, r \triangleright s}{\phi \triangleright \mathrm{natrec}_p^r\ A\ z\ s\ n}$$

$$\begin{array}{rcl}
\mathrm{natrec}_p^r\ A\ z\ s\ \mathrm{zero} & \longrightarrow & z \\
\phi & \leq & \zeta \\
\mathrm{natrec}_p^r\ A\ z\ s\ (\mathrm{suc}\ n) & \longrightarrow & s[n, \mathrm{natrec}_p^r\ A\ z\ s\ n] \\
\phi & \leq & \sigma + p\nu + r\phi
\end{array}$$

$$\begin{array}{lrcl}
\text{Information flow:} & \phi & \leq & \nu \\
\text{Summary:} & \phi & \leq & \underline{\zeta \wedge \nu} \wedge (\underline{\sigma + p\nu} + r\phi) \\
\text{Solution:} & \phi & = & (\zeta \wedge \nu) \circledast_r (\sigma + p\nu)
\end{array}$$

Recursion operator $b \circledast_r s$

$$\frac{\nu \rhd n \qquad \zeta \rhd z \qquad \sigma, p, r \rhd s}{(\zeta \wedge \nu) \circledast_r (\sigma + p\nu) \rhd \mathsf{natrec}^r_p\, A\, z\, s\, n}$$

Recursion:

$$b \circledast_r s \quad \leq \quad b \wedge (s + r \cdot (b \circledast_r s))$$

Interchange with $\_+\_$:

$$(b + b') \circledast_r (s + s') \quad \leq \quad b \circledast_r s + b' \circledast_r s'$$

Distribution with $\_\cdot\_$:

$$(b \circledast_r s) \cdot q \quad \leq \quad bq \circledast_r sq$$

Monotonicity:

$$b \circledast_r s \quad \leq \quad b' \circledast_r s' \text{ when } b \leq b' \text{ and } s \leq s'$$

Erasure modality (completed)

$\omega \leq 0$

$\cdot$	0	ω
0	0	0
ω	0	ω

$+ \quad \wedge \quad \circledast_r$	0	ω
0	0	ω
ω	ω	ω

Erasure

- Keep track of what parts of the program that are used during evaluation
- Remove unneeded parts

$$((\lambda x.\lambda y.x)a)b$$

$\lambda^{\mathbb{N}}$

$$
\begin{aligned}
v, w \ldots ::= {} & x_i \mid \lambda\, t \mid t\, u \\
& \mid \mathsf{zero} \mid \mathsf{suc}\, t \mid \lightning
\end{aligned}
$$

Program extraction

$$\begin{aligned} \mathsf{U}^\bullet &:= \lightning & (t\,^0 u)^\bullet &:= t^\bullet \,\lightning \\ \mathbb{N}^\bullet &:= \lightning & (t\,^\omega u)^\bullet &:= t^\bullet\, u^\bullet \\ (\Pi_p^q\, F\, G)^\bullet &:= \lightning & \mathsf{zero}^\bullet &:= \mathsf{zero} \\ x_i^\bullet &:= x_i & (\mathsf{suc}\, t)^\bullet &:= \mathsf{suc}\, t^\bullet \\ (\lambda^p\, t)^\bullet &:= \lambda\, t^\bullet \end{aligned}$$

$$((\lambda x.\lambda y.x)a)\lightning$$

Logical relation (simplified)

$$\boxed{t \circledR v : \mathsf{U}}$$

$$\frac{\epsilon \vdash t : \mathsf{U}}{t \circledR v : \mathsf{U}}$$

Logical relation (simplified)

$$\boxed{t \circledR v : \mathbb{N}}$$

$$\frac{t \longrightarrow^* \text{zero} \quad v \longrightarrow^* \text{zero}}{t \circledR v : \mathbb{N}}$$

$$\frac{t \longrightarrow^* \text{suc}\, t' \quad v \longrightarrow^* \text{suc}\, v' \quad t' \circledR v' : \mathbb{N}}{t \circledR v : \mathbb{N}}$$

Logical relation (simplified)

$$\boxed{t \circledR v : \Pi_p^q F\, G}$$

$$(\forall a, w.\ a \circledR w : F \Rightarrow t\,^\omega a \circledR v\, w : G[a])$$
$$\Rightarrow t \circledR v : \Pi_\omega^q F\, G$$

$$\big(\forall a, w.\ \epsilon \vdash a : F \Rightarrow t\,^0 a \circledR v\, w : G[a]\big)$$
$$\Rightarrow t \circledR v : \Pi_0^q F\, G$$

Fundamental Lemma

If $\epsilon \vdash t : A$ and $\epsilon \triangleright t$ then t ® $t^{\bullet} : A$.

Conclusion

- Agda formalization at `https://github.com/fhlkfy/logrel-mltt`
- 26.000 loc (1.3MB) Agda sources
- Fork of `https://github.com/mr-ohman/logrel-mltt` (Abel, Öhman, Vezzosi, POPL 2018)
- Several man-months: adding modalities to syntax and reducibility proof (battling slow Agda)
- Further work: other modalities