Analysis-directed semantics

Dominic Orchard
Imperial College London

work in progress

Syntax directed

- e.g. (untyped) λ-calculus ***to*** reduction relation

$$(\lambda x \ . \ e_1) \ e_2 \leadsto e_1 [x / e_2]$$

$$\frac{e_1 \leadsto e_1'}{e_1 \ e_2 \leadsto e_1' \ e_2}$$

Syntax-and-type directed

- e.g. simply-typed λ-calculus *to* CCCs

$$[\ \Gamma \vdash\ e : \tau\ ] \in \mathbf{C}([\Gamma], [\tau]) \qquad \text{i.e.}\ : [\Gamma] \to [\tau]$$

with $[\Gamma] \in \mathbf{C} \quad [\tau] \in \mathbf{C}$

e.g.

$$\frac{\begin{array}{c}[\![\mathit{\Gamma} \vdash e_1 : \sigma \to \tau]\!] = f : [\![\mathit{\Gamma}]\!] \to \tau^\sigma \\ [\![\mathit{\Gamma} \vdash e_2 : \sigma]\!] = g : [\![\mathit{\Gamma}]\!] \to \sigma\end{array}}{[\![\mathit{\Gamma} \vdash e_1\, e_2 : \tau]\!] = \mathsf{app} \circ \langle f, g \rangle : [\![\mathit{\Gamma}]\!] \to \tau}$$

$$\frac{[\![\mathit{\Gamma}, v : \sigma \vdash e : \tau]\!] = f : [\![\mathit{\Gamma}]\!] \times \sigma \to \tau}{[\![\mathit{\Gamma} \vdash \lambda v.e : \sigma \to \tau]\!] = \mathit{\Lambda} f : [\![\mathit{\Gamma}]\!] \to \tau^\sigma}$$

Syntax-and-type directed

$$[\ \Gamma_1 \vdash\ e_1\ :\ t_1\ ] = [\ \Gamma_2 \vdash\ e_2\ :\ t_2\ ] \Rightarrow\ t_1 = t_2\ \wedge\ \Gamma_1 = \Gamma_2$$

see signature of interpretation

$$[\_] : (e : \mathrm{term})$$

syntax

(Syntax-and-)analysis directed

$$[\_] : (e : \mathrm{term}) * (i : \mathrm{analysis}(e)) \to D\ i$$

- e.g. simple-typed λ-calculus with <u>effect system</u>

$$[\ \Gamma \vdash\ e : \tau,\ \mathsf{F}\ ]\ \in\ (\Gamma \to \mathrm{T}\ \mathsf{F}\ \tau)$$

Constructing analysis-directed semantics

- Analysis domain A, semantic domain D
- Define $\mathrm{F} : \mathrm{A} \to \mathrm{D}$ to be structure preserving (homomorphism) between A and D
- Gives a design framework for A and D
- Equations in A map to equations in D

Context

- Work on coeffects (with Tomas Petricek & Alan Mycroft)

$$[\![\Gamma \mathrel{?} \mathrm{R} \vdash e : \tau]\!] \in \mathbf{C}(\mathrm{D}_{\mathrm{R}}[\![\Gamma]\!], [\![\tau]\!])$$

  - "A core quantitative coeffect calculus" (Brunel, Gaboardi, Mazza, Zdancewic), ESOP 2013
  - "Bounded linear types" (Ghica and Smith), ESOP 2013

- Work on effects (Shinya Katsumata, 'parametric effect monads')

$$[\![\Gamma \vdash e : \tau \mathrel{!} \mathrm{F}]\!] \in \mathbf{C}([\![\Gamma]\!], \mathrm{M}_{\mathrm{F}}[\![\tau]\!])$$

- All define *analysis-directed semantics* (and leverage this for soundness)

Effect systems

$\boxed{\Gamma \vdash e : \tau,\ \mathsf{F}}$ $\boxed{\text{monoid} \quad (\mathsf{F}, \sqcup, \varnothing)}$

$$[\text{abs}]\ \frac{\Gamma, x : \sigma \vdash e : \tau,\ \mathsf{F}}{\Gamma \vdash \lambda x\,.\,e : \sigma \xrightarrow{\mathsf{F}} \tau,\ \varnothing}$$

$$[\text{var}]\ \frac{x : \sigma \in \Gamma}{\Gamma \vdash x : \sigma,\ \varnothing}$$

$$[\text{app}]\ \frac{\Gamma \vdash e_1 : \sigma \xrightarrow{\mathsf{F}} \tau,\ \mathsf{G} \qquad \Gamma \vdash e_2 : \sigma,\ \mathsf{H}}{\Gamma \vdash e_1\, e_2 : \tau,\ \mathsf{G} \sqcup \mathsf{H} \sqcup \mathsf{F}}$$

$$[\text{write}]\ \frac{\Gamma \vdash e : \tau,\ \mathsf{F} \qquad (x : \mathit{ref}\ \tau) \in \Gamma}{\Gamma \vdash x := e : (),\ \mathsf{F} \cup \{\mathrm{W}(x)\}}$$

$$[\text{read}]\ \frac{(x : \mathit{ref}\ \tau) \in \Gamma}{\Gamma \vdash !x : \tau,\ \{\mathrm{R}(x)\}}$$

Effect systems married to monads

$\Gamma \vdash e : \mathrm{T}\ \mathsf{F}\ \tau$

monoid $(\mathsf{F}, \sqcup, \varnothing)$

[abs] $$\frac{\Gamma, x : \sigma \vdash e : \mathrm{T}\ \mathsf{F}\ \tau}{\Gamma \vdash \lambda x\ .\ e : \mathrm{T}\ \varnothing\ (\sigma \to \mathrm{T}\ \mathsf{F}\ \tau)}$$

[var] $$\frac{x : \sigma \in \Gamma}{\Gamma \vdash x : \mathrm{T}\ \varnothing\ \sigma}$$

[app] $$\frac{\Gamma \vdash e_1 : \mathrm{T}\ \mathsf{G}\ (\sigma \to \mathrm{T}\ \mathsf{F}\ \tau) \qquad \Gamma \vdash e_2 : \mathrm{T}\ \mathsf{H}\ \sigma}{\Gamma \vdash e_1\, e_2 : \mathrm{T}\ (\mathsf{G} \sqcup \mathsf{H} \sqcup \mathsf{F})\ \tau}$$

“The marriage of effects and monads” (Wadler & Thiemann, 2003)

Unifying effect-analysis and semantics

	$M : [C,\ C]$	$F : \mathbf{Set}$	monoid homomorphism $T : F \to [C,\ C]$
seq	$\mu : M \circ M \to M$	$\sqcup : F \times F \to F$	$\mathrm{T}\ \mathrm{F} \circ \mathrm{T}\ \mathrm{G} = \mathrm{T}\ (\mathrm{F} \sqcup \mathrm{G})$
id	$\eta : 1_C \to M$	$\varnothing : 1 \to F$	$1_C = \mathrm{T}\ \varnothing$

$$
\begin{tikzcd}
\mathcal{F} \times \mathcal{F} \arrow[rr, "\sqcup"] \arrow[d, "T \times T"'] & & \mathcal{F} \arrow[d, "T"] \\
{[\mathcal{C},\mathcal{C}] \times [\mathcal{C},\mathcal{C}]} \arrow[rr, "\circ"'] \arrow[urr, phantom, "\Nearrow \mu"] & & {[\mathcal{C},\mathcal{C}]}
\end{tikzcd}
\qquad
\begin{tikzcd}
1 \arrow[r, "\emptyset"] \arrow[dr, bend right, "id"'] & \mathcal{F} \arrow[d, "T"] \\
& {[\mathcal{C},\mathcal{C}]} \arrow[ul, phantom, "\Nearrow \eta"]
\end{tikzcd}
$$

$$\mu_{F,G} : T_F \circ T_G \to T_{(F \sqcup G)} \qquad \eta_\varnothing : 1 \to T_\varnothing$$

Katsumata, Parametric Effect Monads and Semantics of Effect Systems, POPL 2014

Equations

- Identities preserved (trivial)

$$\mathrm{T}\ \mathrm{F} = \mathrm{T}\ (\mathrm{F} \sqcup \varnothing) = \mathrm{T}\ \mathrm{F} \circ \mathrm{T}\varnothing = \mathrm{T}\ \mathrm{F} \circ 1 = \mathrm{T}\ \mathrm{F}$$

- For lax, have the diagram:

$$\begin{tikzcd}
T_{F \sqcup \emptyset} & T_F \arrow[l, "T\rho"'] \arrow[d, "\rho"] \\
T_F \circ T_\emptyset \arrow[u, "\mu_{F,\emptyset}"] & T_F \circ 1_{\mathcal{C}} \arrow[l, "T_F \circ \eta_\emptyset"]
\end{tikzcd}$$

- For strict monoids…

analogues of monad laws

$$\begin{tikzcd}
T_F & \\
T_F T_\emptyset \arrow[u, "\mu_{F,\emptyset}"] & T_F \arrow[l, "T_F \eta_\emptyset"] \arrow[ul, equal]
\end{tikzcd}$$

Corresponding equations

$$[\,\Gamma_1 \vdash e_1 : t_1, \mathrm{F}] = [\,\Gamma_2 \vdash e_2 : t_2, \mathrm{G}\,]$$
$$\Rightarrow\ t_1 = t_2 \ \wedge\ \Gamma_1 = \Gamma_2 \wedge (\mathrm{F} = \mathrm{G})$$

- When considering equations on semantics

$$[\,\Gamma_1 \vdash e_1 : t_1, \mathrm{F}] \stackrel{?}{=} [\,\Gamma_2 \vdash e_2 : t_2, \mathrm{G}\,]$$

proof tree for (F = G) implies semantic laws

- e.g. $[\,\Gamma_1 \vdash e_1 : t_1, \mathrm{F} \sqcup \varnothing] = [\,\Gamma_2 \vdash e_2 : t_2, \mathrm{F}\,]$

$$\Rightarrow \begin{tikzcd} T_F & \\ T_F T_\emptyset \arrow[u, "\mu_{F,\emptyset}"] & T_F \arrow[l, "T_F \eta_\emptyset"] \arrow[ul, equal] \end{tikzcd}$$

if η is the only way to introduce $\varnothing$

Bounded linear logic analysis

Reuse bounds on free-variables $x : \sigma \mathrel{?} \mathbf{n}$

- Core rules (with sub-coeffects)

$$\text{[abs]}\ \frac{\Gamma, x : \sigma \mathrel{?} \mathsf{s} \vdash e : \tau}{\Gamma \vdash \lambda x.e : \sigma \xrightarrow{\mathsf{s}} \tau} \qquad \text{[var]}\ \frac{}{x : \sigma \mathrel{?} 1 \vdash x : \sigma}$$

$$\text{[app]}\ \frac{\Gamma_1 \vdash e_1 : \sigma \xrightarrow{\mathsf{s}} \tau \qquad \Gamma_2 \vdash e_2 : \sigma}{\Gamma_1, \mathsf{s} \mathbin{\underline{*}} \Gamma_2 \vdash e_1\, e_2 : \tau}$$

- Specialised structural rules

$$\text{[weak]}\ \frac{\Gamma \vdash e : \tau}{\Gamma, x : \sigma \mathrel{?} \mathbf{0} \vdash e : \tau} \qquad \text{[contr]}\ \frac{\Gamma_1, x : \sigma \mathrel{?} \mathbf{a},\ y : \sigma \mathrel{?} \mathbf{b}, \Gamma_2 \vdash e : \tau}{\Gamma_1,\ z : \sigma \mathrel{?} \mathbf{a+b},\ \Gamma_2 \vdash e[z/x, z/y] : \tau}$$

Bounded linear logic analysis

$$(\lambda v.x+v+v)\ (x+y)$$

$$\dfrac{\text{(abs)}\ \dfrac{x:\mathbb{Z}, v:\mathbb{Z}?\langle 1,2\rangle \vdash x+v+v:\mathbb{Z}}{x:\mathbb{Z}?\langle 1\rangle \vdash (\lambda v.x+v+v):\mathbb{Z}\xrightarrow{2}\mathbb{Z}} \qquad \dfrac{\vdots}{x':\mathbb{Z}, y:\mathbb{Z}?\langle 1,1\rangle \vdash x'+y:\mathbb{Z}}}{\text{(contr)}\ \dfrac{(\equiv)\ \dfrac{\text{(app)}\ x:\mathbb{Z}, x':\mathbb{Z}, y:\mathbb{Z}?\langle 1\rangle \times (2*\langle 1,1\rangle) \vdash (\lambda v.x+v+v)\ (x'+y):\mathbb{Z}}{x:\mathbb{Z}, x':\mathbb{Z}, y:\mathbb{Z}?\langle 1,2,2\rangle \vdash (\lambda v.x+v+v)\ (x'+y):\mathbb{Z}}}{x:\mathbb{Z}, y:\mathbb{Z}?\langle 3,2\rangle \vdash (\lambda v.x+v+v)\ (x+y):\mathbb{Z}}}$$

$$(\lambda v.x+v+v)\ (x+y) \ \rightsquigarrow_\beta\ x+(x+y)+(x+y)$$

$$x:\mathbb{Z}, y:\mathbb{Z}?\langle 3,2\rangle \vdash x+(x+y)+(x+y):\mathbb{Z}$$

BLL-directed semantics

- Bounded reuse (exponent) $\mathrm{D}n\ A = A^n = \langle A_1,..,A_n \rangle$

$$\mathrm{D} : \mathbb{N} \to [\mathbf{C},\mathbf{C}]$$

- Monoid and scalar-vector multiplication (monoid action) on $\mathbb{N}$

$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ contraction

$0 : 1 \to \mathbb{N}$ weakening

$1 : 1 \to \mathbb{N}$ variables

$\underline{*} : \mathbb{N} \times \mathbb{N}^n \to \mathbb{N}^n$ composition

$* : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$\frac{\Gamma_1 \vdash e_1 : \sigma \xrightarrow{s} \tau \qquad \Gamma_2 \vdash e_2 : \sigma}{\Gamma_1,\ s\ \underline{*}\ \Gamma_2 \vdash e_1\ e_2 : \tau}$$

$$s\ \underline{*}\ (x_1 : t_1\ ?\ r_1,\ \ldots,\ x_n : t_n\ ?\ r_n) = x_1 : t_1\ ?\ s * r_1,\ \ldots,\ x_n : t_n\ ?\ s * r_n$$

will treat as a vector $s\ \underline{*} \langle r_1, \ldots, r_n \rangle = \langle s * r_1, \ldots, s * r_n \rangle$

BLL-directed semantics

- Structure preserving $D : \mathbb{N} \to [\mathbf{C},\mathbf{C}]$

$$
\begin{tikzcd}
s \,\underline{*}\, \langle r_1, \ldots, r_n \rangle \arrow[r, mapsto, dotted] \arrow[dd, mapsto, dotted] & \langle s * r_1, \ldots, s * r_n \rangle \arrow[d, mapsto, dotted] \\
 & \langle D_{(s * r1)}, \ldots, D_{(s * rn)} \rangle \arrow[d, "\delta^n"] \\
D_s \times \langle D_{r1}, \ldots, D_{rn} \rangle \arrow[r, mapsto, dotted] & \langle D_sD_{r1}, \ldots, D_sD_{rn} \rangle
\end{tikzcd}
$$

$$
\begin{tikzcd}
\mathbb{N} \times \mathbb{N}^n \arrow[r, "\underline{*}"] \arrow[d, "D \times D^n"'] & \mathbb{N}^n \arrow[d, "D^n"] \arrow[dl, "\delta^n"] \\
{[\mathbf{C},\mathbf{C}] \times [\mathbf{C},\mathbf{C}]^n} \arrow[r, "\circ^n"'] & {[\mathbf{C},\mathbf{C}]^n}
\end{tikzcd}
$$

$$\delta^n : (D_{(s * r1)} \times \ldots \times D_{(s * rn)}) \to (D_sD_{r1} \times \ldots \times D_sD_{rn})$$

BLL-directed semantics

$$\delta^n : (D_{(s * r1)} \times \ldots \times D_{(s * rn)}) \rightarrow (D_s D_{r1} \times \ldots \times D_s D_{rn})$$

- Coeffect-parameterised comonad

$$\delta : D_{s*r}\, A \rightarrow D_s D_r\, A$$

“s*r copies turned into s copies of r copies”

$$\varepsilon : D_1\, A \rightarrow A$$

“use one copy”

Coeffect-directed semantics

$$[\text{contr}]\quad \frac{\Gamma_1, x : \sigma \mathbin{?} \textsf{a},\ y : \sigma \mathbin{?} \textsf{b}, \Gamma_2 \vdash e : \tau}{\Gamma_1,\ z : \sigma \mathbin{?} \textsf{a+b}, \Gamma_2 \vdash e : \tau}$$

$$\begin{tikzcd}
(\mathbb{N} \times \mathbb{N}) \arrow[rr, "D \times D"] \arrow[d, "+"'] & & {[\mathbf{C},\mathbf{C}] \times [\mathbf{C},\mathbf{C}]} \arrow[d, "{<_,\ _>}"] \arrow[dl, "m"] \\
\mathbb{N} \arrow[rr, "D"'] & {} & {[\mathbf{C},\ \mathbf{C}]}
\end{tikzcd}$$

$$\Delta_{r,s} : D_{(r+s)}\, A \to D_r\, A \times D_s\, A$$

Coeffect-directed semantics

BLL analysis

$$[\text{abs}]\ \frac{\Gamma,\, x : \sigma \,?\, \mathsf{s} \vdash e : \tau}{\Gamma \vdash \lambda x.e : \sigma \xrightarrow{\mathsf{s}} \tau}$$

… as coeffect analysis

$$[\text{abs}]\ \frac{\Gamma,\, x : \sigma \,?\, \mathsf{R} \times \langle \mathsf{s} \rangle \vdash e : \tau}{\Gamma ?\, \mathsf{R} \vdash \lambda x.e : \sigma \xrightarrow{\mathsf{s}} \tau}$$

in general

one 'shaped' annotation

$$[\text{abs}]\ \frac{\Gamma,\, x : \sigma \,?\, \mathsf{R} \sqcap \langle \mathsf{s} \rangle \vdash e : \tau}{\Gamma ?\, \mathsf{R} \vdash \lambda x.e : \sigma \xrightarrow{\mathsf{s}} \tau}$$

e.g. distributed resources

$$[\text{abs}]\ \frac{\Gamma,\, x : \sigma \,?\, \{\mathsf{gps}, \mathsf{db}\} \vdash e : \tau}{\Gamma ?\, \{\mathsf{db}\} \vdash \lambda x.e : \sigma \xrightarrow{\mathsf{gps}} \tau}$$

Coeffect-directed semantics

$$[\text{abs}]\quad \frac{\Gamma, x : \sigma \mathrel{?} R \sqcap \langle s \rangle \vdash e : \tau}{\Gamma \mathrel{?} R \vdash \lambda x.e : \sigma \xrightarrow{s} \tau}$$

let $D' = \mathit{uncurry}\ D$ **i.e.** $D' : \mathbb{I} \times \mathbf{C} \to \mathbf{C}$

$\bowtie$ composes binary ops

$$\begin{tikzcd}
(\mathbb{I} \times \mathbf{C}) \times (\mathbb{I} \times \mathbf{C}) \arrow[r, "D' \times D'"] \arrow[d, "\sqcap \bowtie \times"'] & \mathbf{C} \times \mathbf{C} \arrow[d, "\times"] \arrow[dl, "m"] \\
\mathbb{I} \times \mathbf{C} \arrow[r, "D'"'] & \mathbf{C}
\end{tikzcd}$$

$$m_{r,s} : D_r\, A \times D_s\, B \to D_{(r \sqcap s)} (A \times B)$$

Constructing analysis-directed semantics

- Analysis domain A, semantic domain D
- Define $\mathrm{F} : \mathrm{A} \to \mathrm{D}$ to be structure preserving (homomorphism) between A and D
- Gives a design framework for A and D
- Equations in A map to equations in D

Corresponding equations

- Use algebraic solver on analysis domain A (e.g., I use Prover 9)
- Rest of proof not corresponding to A usually naturally and universality
- Tactic generator!
- Build into theorem prover?

Thanks!

http://dorchard.co.uk