Datafun: Semantics

Neel Krishnaswami
University of Cambridge

FLOLAC 2024
Taipei, Taiwan

The Design Invariant

If $\cdot ; \cdot \vdash f : \{E\} \longrightarrow \{E\}$

then f is a monotone function

Posets

A partially ordered set is

$$(X \in \mathrm{Set}, (\sqsubseteq) \subseteq X \times X)$$

s.t. $\forall x \in X. \quad x \sqsubseteq x$

$\forall x, y.$ if $x \sqsubseteq y$ and $y \sqsubseteq x$ then $x = y$

$\forall x, y, z.$ if $x \sqsubseteq y$ and $y \sqsubseteq z$ then $x \sqsubseteq z$

Monotone Functions

If $(X, \sqsubseteq_X)$ and $(Y, \sqsubseteq_Y)$ are posets

$f : X \longrightarrow Y$ is <u>monotone</u> when

$\forall\, x, x' \in X .$ if $x \sqsubseteq_X x'$ then $f(x) \sqsubseteq_Y f(x')$

New Posets from Old

If E is a finite set, then

$(\mathcal{P}(E), \subseteq)$ is a poset

New Posets from Old

If $(X, \sqsubseteq_X)$ and $(Y, \sqsubseteq_Y)$ are posets

$$(X, \sqsubseteq_X) \times (Y, \sqsubseteq_Y) = (X \times Y, \sqsubseteq_{X \times Y})$$

where

$$(x, y) \sqsubseteq_{X \times Y} (x', y') \text{ iff } x \sqsubseteq_X x' \text{ and } y \sqsubseteq_Y y'$$

New Posets from Old

$\mathbb{1} = (\{*\}, \leq_1)$ is a poset

where

$$* \leq_1 *$$

New Posets from Old

If $(X, \sqsubseteq_X)$ and $(Y, \sqsubseteq_Y)$ are posets

$$(X, \sqsubseteq_X) + (Y, \sqsubseteq_Y) = (X+Y, \sqsubseteq_{X+Y})$$

where

$$in_1(x) \sqsubseteq_{X+Y} in_1(x') \quad \text{iff} \quad x \sqsubseteq_X x'$$

$$in_2(y) \sqsubseteq_{X+Y} in_2(y') \quad \text{iff} \quad y \sqsubseteq_Y y'$$

New Posets from Old

If $(X, \sqsubseteq_X)$ and $(Y, \sqsubseteq_Y)$ are posets

$$(X, \sqsubseteq_X) \to (Y, \sqsubseteq_Y) = (X \longrightarrow Y, \sqsubseteq_{X \to Y})$$

where $f \sqsubseteq_{X \to Y} f'$ iff

$$\forall x, x'.\ \text{if } x \sqsubseteq_X x' \text{ then } f(x) \sqsubseteq_Y f'(x')$$

New Posets from Old

If $(X, \sqsubseteq_X)$ is a poset

$\square(X, \sqsubseteq) = (X, =_X)$ is a poset

This replaces the partial order with equality, making the order discrete

The Strategy

1. Associate a poset to each type
2. Associate a poset to the context
3. Show that each $\Delta; \Gamma \vdash e : A$ is monotone

(4. Learn denotational semantics)

Syntax

Types $\quad A, B ::= 1 \mid A \times B \mid A \to B \mid A + B \mid \{E\} \mid \Box A$

Eq types $\quad E, F ::= 1 \mid E + F \mid E \times F \mid \{E\}$

$\Gamma ::= \cdot \mid \Gamma, x : A \qquad \Delta ::= \cdot \mid \Delta, x : A$

$$
\begin{aligned}
e ::= \; & () \mid (e, e') \mid \pi_i(e) \mid \lambda x . e \mid e\, e' \mid in_i(e) \\
& \mid case\,(e, \overrightarrow{in_i\, x_i \to e_i}) \mid \emptyset \mid e \cup e' \mid for\ x \in e . e' \mid \{e\} \\
& \mid box(e) \mid let\ box(x) = e\ in\ e' \\
& \mid fix\ x : L . e \mid x \mid \underline{x} \mid e_1 = e_2 \mid empty?(e)
\end{aligned}
$$

$$\boxed{\Delta ; \Gamma \vdash e : A}$$

Typing

$$\frac{x : A \in \Gamma}{\Delta ; \Gamma \vdash x : A} \qquad \frac{}{\Delta ; \Gamma \vdash () : 1} \qquad \frac{\Delta ; \Gamma \vdash e_1 : A_1 \quad \Delta ; \Gamma \vdash e_2 : A_2}{\Delta ; \Gamma \vdash (e_1 , e_2) : A_1 \times A_2}$$

$$\frac{\Delta ; \Gamma \vdash e : A_1 \times A_2}{\Delta ; \Gamma \vdash \pi_i (e) : A_i} \qquad \frac{\Delta ; \Gamma , x : A \vdash e : B}{\Delta ; \Gamma \vdash \lambda x . e : A \to B} \qquad \frac{\Delta ; \Gamma \vdash e_1 : A \to B \quad \Delta ; \Gamma \vdash e_2 : A}{\Delta ; \Gamma \vdash e_1 \, e_2 : B}$$

$$\frac{\Delta ; \Gamma \vdash e : A_i}{\Delta ; \Gamma \vdash in_i (e) : A_1 + A_2} \qquad \frac{\Delta ; \Gamma \vdash e : A_1 + A_2 \quad \Delta ; \Gamma , x_1 : A_1 \vdash e_1 : B \quad \Delta ; \Gamma , x_2 : A_2 \vdash e_2 : B}{\Delta ; \Gamma \vdash case (e , in_1 \, x_1 \to e_1 , in_2 \, x_2 \to e_2) : B}$$

Modal Typing

$$\frac{x : A \in \Delta}{\Delta ; \Gamma \vdash \underline{x} : A}$$

$$\frac{\Delta ; \cdot \vdash e : A}{\Delta ; \Gamma \vdash \mathrm{box}(e) : \Box A}$$

$$\frac{\Delta ; \Gamma \vdash e_1 : \Box A \qquad \Delta , x : A ; \Gamma \vdash e_2 : B}{\Delta ; \Gamma \vdash \mathrm{let}\ \mathrm{box}(x) = e_1\ \mathrm{in}\ e_2 : B}$$

Data Structures

$$\boxed{E, F ::= 1 \mid E + F \mid E \times F \mid \{E\}}$$

$$\frac{\Delta; \cdot \vdash e : E}{\Delta; \Gamma \vdash \{e\} : \{E\}}$$

$$\frac{}{\Delta; \Gamma \vdash \phi : \{E\}}$$

$$\frac{\Delta; \Gamma \vdash e_1 : \{E\} \quad \Delta; L \vdash e_2 : \{E\}}{\Delta; \Gamma \vdash e_1 \cup e_2 : \{E\}}$$

$$\frac{\Delta; x : \{E\} \vdash e : \{E\}}{\Delta; \Gamma \vdash \mathrm{fix}\ x.\ e : \{E\}}$$

$$\frac{\Delta; \Gamma \vdash e_1 : \{E\} \quad \Delta, x : E; \Gamma \vdash e_2 : \{F\}}{\Delta; \Gamma \vdash \mathrm{for}\ x \in e_1 .\ e_2 : \{F\}}$$

$$\frac{\Delta; \cdot \vdash e_1 : E \quad \Delta; \cdot \vdash e_2 : E}{\Delta; \Gamma \vdash e_1 = e_2 : \mathrm{bool}}$$

$$\frac{\Delta; \cdot \vdash e : \{1\}}{\Delta; \cdot \vdash \mathrm{empty?} : \mathrm{bool}}$$

$1 + 1$

A Poset For Each Type

$$[\![-]\!] : \text{Type} \to \text{Poset}$$

$$[\![1]\!] = 1$$
$$[\![A \times B]\!] = [\![A]\!] \times [\![B]\!]$$
$$[\![A + B]\!] = [\![A]\!] + [\![B]\!]$$
$$[\![X \to Y]\!] = [\![X]\!] \to [\![Y]\!]$$
$$[\![\Box A]\!] = \Box [\![A]\!]$$
$$[\![\{E\}]\!] = \text{let } (\hat{E}, \sqsubseteq) = [\![E]\!] \text{ in } (\mathcal{P}(\hat{E}), \subseteq)$$

A Poset for the Context

$[\![\cdot]\!] = 1$

$[\![\Gamma, x : A]\!] = [\![\Gamma]\!] \times [\![A]\!]$

These have order

$[\![\cdot]\!] = 1$

$[\![\Delta, x : A]\!] = [\![\Delta]\!] \times \Box [\![A]\!]$

These are discrete

An Observation

The set $\square(A, \sqsubseteq_A) \to (B, \sqsubseteq_B)$ is just the regular functions $A \to B$

Suppose $f \in A \to B$

To show it is monotone at $\square(A, \sqsubseteq_A) \to (B, \sqsubseteq_B)$

WTS $\forall x, x'.$ if $x = x'$ then $f(x) \sqsubseteq f(x')$

But this is trivial!

An Observation

The set $\square(A, \sqsubseteq_A) \to (B, \sqsubseteq_B)$ is just the regular functions $A \to B$

Suppose $f \in A \to B$

To show it is monotone at $\square(A, \sqsubseteq_A) \to (B, \sqsubseteq_B)$

WTS $\forall x, x'.$ if $x = x'$ then $f(x) = f(x')$

But this is trivial!

$\boxed{\text{So } \square A \text{ gives us the usual functions.}}$

The Semantics

If $\Delta ; \Gamma \vdash e : A$ then

$$[\![\Delta ; \Gamma \vdash e : A]\!] \in [\![\Delta]\!] \times [\![\Gamma]\!] \to_m [\![A]\!]$$

monotone

Theorem:

If $(\delta, \gamma) \sqsubseteq (\delta', \gamma')$ then

$$[\![\Delta ; \Gamma \vdash e : A]\!] (\delta, \gamma) \sqsubseteq [\![\Delta ; \Gamma \vdash e : A]\!] (\delta', \gamma')$$

The Semantics

$$\left[\!\left[\frac{x_i : A \in \Gamma}{\Delta ; \Gamma \vdash x_i : A} \right]\!\right] (\delta, \gamma) = \pi_i (\gamma)$$

$$[\![\Delta ; \Gamma \vdash () : 1]\!] (\delta, \gamma) = *$$

$$[\![\Delta ; \Gamma \vdash (e_1, e_2) : A \times B]\!] (\delta, \gamma) =$$

$$\begin{aligned} &\text{let } a = [\![\Delta ; \Gamma \vdash e_1 : A]\!] (\delta, \gamma) \\ &\text{let } b = [\![\Delta ; \Gamma \vdash e_2 : B]\!] (\delta, \gamma) \\ &(a, b) \end{aligned}$$

$$[\![x : A , y : B , z : C]\!]$$

$$((1 \times A) \times B) \times C$$

$$\pi_x(\gamma) = \pi_1(\pi_1(\pi_2 \, \gamma))$$

If $(\delta, \gamma) \sqsubseteq (\delta', \gamma')$

then $\delta = \delta'$

The Semantics

$$[\![\Delta ; \Gamma \vdash \pi_i (e) : A_i]\!] (\delta, \gamma) =$$

$$\text{let } (a_1, a_2) = [\![\Delta ; \Gamma \vdash e : A_1 \times A_2]\!] (\delta, \gamma) \text{ in}$$

$$a_i$$

$$[\![\Delta ; \Gamma \vdash \lambda x . e : A \to B]\!] (\delta, \gamma) =$$

$$\lambda a \in [\![A]\!] . \ [\![\Delta ; \Gamma , x : A \vdash e : B]\!] (\delta, (\gamma, a))$$

$$[\![\Delta ; \Gamma \vdash e_1 \, e_2 : B]\!] (\delta, \gamma) =$$

$$\text{let } f = [\![\Delta ; \Gamma \vdash e_1 : A \to B]\!] (\delta, \gamma) \text{ in}$$

$$\text{let } a = [\![\Delta ; \Gamma \vdash e_2 : A]\!] (\delta, \gamma) \text{ in}$$

$$f(a)$$

$$\overbrace{\left(\lambda a \in [\![A]\!].\ [\![\Delta; \Gamma, x : A \vdash e : B]\!](\delta, (\gamma, a))\right)}^{F}$$

If $\gamma \sqsubseteq \gamma'$

$$\sqsubseteq_{[\![A]\!] \to [\![B]\!]}$$

$$\underbrace{\left(\lambda a \in [\![A]\!].\ [\![\Delta; \Gamma, x : A \vdash e : B]\!](\delta, (\gamma', a))\right)}_{F'}$$

$$\forall a \sqsubseteq a'.\ F a \sqsubseteq F' a'$$

$$[\![\Delta; \Gamma, x : A \vdash e : B]\!](\delta, (\gamma, a)) \sqsubseteq_B$$

$$[\![\Delta; \Gamma, x : A \vdash e : B]\!](\delta, (\gamma', a'))$$

$\gamma \sqsubseteq \gamma'$

$a \sqsubseteq a'$

$(\gamma, a) \sqsubseteq (\gamma', a')$

The Semantics

$$[\![\Delta; \Gamma \vdash \mathrm{in}_i(e) : A_1 + A_2]\!](\delta, \gamma) =$$
$$\quad \mathrm{let}\ v = [\![\Delta; \Gamma \vdash e : A_i]\!](\delta, \gamma)\ \mathrm{in}$$
$$\quad\quad \amalg_i(v)$$

$$[\![\Delta; \Gamma \vdash \mathrm{case}(e, \overrightarrow{\mathrm{in}_i\, x_i \to e_i}) : B]\!](\delta, \gamma) =$$
$$\quad \mathrm{let}\ v = [\![\Delta; \Gamma \vdash e : A_1 + A_2]\!](\delta, \gamma)\ \mathrm{in}$$
$$\quad\quad \begin{cases} [\![\Delta; \Gamma, x_1 : A_1 \vdash e_1 : B]\!](\delta, (\gamma, v')) & \text{when } v = \amalg_1 v' \\ [\![\Delta; \Gamma, x_2 : A \vdash e_2 : B]\!](\delta, (\gamma, v')) & \text{when } v = \amalg_2 v' \end{cases}$$

The Semantics

$$\left[\!\left[\frac{x_i : A_i \in \Delta}{\Delta ; \Gamma \vdash \underline{x_i} : A_i} \right]\!\right] (\delta, \gamma) = \pi_i (\delta)$$

$$\left[\!\left[\Delta ; \Gamma \vdash \mathrm{box}(e) : \Box A \right]\!\right] (\delta, \gamma) =$$

$$\left[\!\left[\Delta ; \cdot \vdash e : A \right]\!\right] (\delta, *)$$

$$\left[\!\left[\Delta ; \Gamma \vdash \mathrm{let}\ \mathrm{box}(x) = e_1\ \mathrm{in}\ e_2 : B \right]\!\right] (\delta, \gamma) =$$

$$\mathrm{let}\ a = \left[\!\left[\Delta ; \Gamma \vdash e_1 : \Box A \right]\!\right] (\delta, \gamma)\ \mathrm{in}$$

$$\left[\!\left[\Delta , x : A ; \Gamma \vdash e_2 : B \right]\!\right] ((\delta, a), \gamma)$$

The Semantics

$$[\![\Delta ; \Gamma \vdash \{e\} : \{E\}]\!] (\delta, \gamma) = \{ [\![\Delta ; \cdot \vdash e : E]\!] (\delta, *) \}$$

$$[\![\Delta ; \Gamma \vdash \emptyset : \{E\}]\!] (\delta, \gamma) = \{\}$$

$$[\![\Delta ; \Gamma \vdash e_1 \cup e_2 : \{E\}]\!] (\delta, \gamma) =$$

$$\begin{aligned} &\text{let } X = [\![\Delta ; \Gamma \vdash e_1 : \{E\}]\!] (\delta, \gamma) \text{ in} \\ &\text{let } Y = [\![\Delta ; \Gamma \vdash e_2 : \{E\}]\!] (\delta, \gamma) \text{ in} \\ &X \cup Y \end{aligned}$$

$$[\![\Delta ; \Gamma \vdash e_1 = e_2 : \text{bool}]\!] (\delta, \gamma) =$$

$$\begin{aligned} &\text{let } v_1 = [\![\Delta ; \cdot \vdash e_1 : E]\!] (\delta, *) \text{ in} \\ &\text{let } v_2 = [\![\Delta ; \cdot \vdash e_2 : E]\!] (\delta, *) \text{ in} \\ &v_1 = v_2 \end{aligned}$$

The Semantics

$$[\![\Delta ; \Gamma \vdash \{e\} : \{E\}]\!] (\delta, \gamma) = \{ [\![\Delta ; \cdot \vdash e : E]\!] (\delta, *) \}$$

$$[\![\Delta ; \Gamma \vdash \emptyset : \{E\}]\!] (\delta, \gamma) = \{\}$$

$$[\![\Delta ; \Gamma \vdash e_1 \cup e_2 : \{E\}]\!] (\delta, \gamma) =$$

$$\begin{aligned} & \text{let } X = [\![\Delta ; \Gamma \vdash e_1 : \{E\}]\!] (\delta, \gamma) \text{ in} \\ & \text{let } Y = [\![\Delta ; \Gamma \vdash e_2 : \{E\}]\!] (\delta, \gamma) \text{ in} \\ & X \cup Y \end{aligned}$$

The Semantics

$$
\llbracket \Delta; \Gamma \vdash \text{for } x \in e_1 .\, e_2 : \{F\} \rrbracket (\delta, \gamma) =
$$

$$
\text{let } X = \llbracket \Delta; \Gamma \vdash e_1 : \{E\} \rrbracket (\delta, \gamma) \text{ in}
$$

$$
\bigcup_{v \in X} \llbracket \Delta, x : E; \Gamma \vdash e_2 : \{F\} \rrbracket ((\delta, v), \gamma)
$$

$$
\llbracket \Delta; \Gamma \vdash \text{fix } x . e : \{E\} \rrbracket (\delta, \gamma) =
$$

$$
\text{let } F = \lambda X \in \llbracket \{E\} \rrbracket .\, \llbracket \Delta; \underbrace{x : \{E\}}_{1 \times \mathcal{P}(\llbracket E \rrbracket)} \vdash e : \{E\} \rrbracket (\delta, (*, X))
$$

$$
\mathrm{lfp}(F)
$$

Denotational vs. Operational

- In this case, we used a denotational semantics
- Operational semantics is also possible (but messier)