From semantics to types: the case of the imperative λ-calculus

Ugo de'Liguoro, Riccardo Treglia

University of Turin, Italy

MFPS XXXVII - Salzburg, 30 August - 3 September 2021

Overview

Overview

Goal: to find a type assignment system to reason about functional programs with side-effects

Overview

Goal: to find a type assignment system to reason about functional programs with side-effects

Approach: Moggi's idea of modeling effectful computations using monads

Overview

Goal: to find a type assignment system to reason about functional programs with side-effects

Approach: Moggi's idea of modeling effectful computations using monads

Background: computational core λ_c + Intersection Types

Overview

Goal: to find a type assignment system to reason about functional programs with side-effects

Approach: Moggi's idea of modeling effectful computations using monads

Background: computational core λ_c + Intersection Types

Contents:

- definition of λ_{imp} out of a domain equation
- solution of the equation as a **filter model**;
- derivation of a **type assignment system** out of the interpretation of terms as filters of types

Overview

Goal: to find a type assignment system to reason about functional programs with side-effects

Approach: Moggi's idea of modeling effectful computations using monads

Background: computational core λ_c + Intersection Types

Contents:
- definition of λ_{imp} out of a domain equation
- solution of the equation as a **filter model**;
- derivation of a **type assignment system** out of the interpretation of terms as filters of types

In this paper:
Denotational Semantics of λ_{imp}
and its type system

In a companion paper:
Operational Semantics of λ_{imp}
(soon in PPDP'21)

Modeling effects by monads

To model computational effects, Moggi (1991) proposed **monads** (here in Wadler's type theoretic formulation)

$$(T, unit, \star)$$

where

$$\begin{array}{lcl} T A & = & \text{the type of } \textbf{computations} \text{ over values of type } A \\ unit\ V & = & \text{the trivial computation returning the } \textbf{value } V \\ M \star F & = & \text{the application to the computation } M \text{ of } F^\dagger : T A \to T B \\ & & \text{that is the (unique) extension of } F : A \to T B \text{ s.t.} \end{array}$$

$$F^\dagger(unit\ V) = F\ V$$

$$\frac{V : A}{unit\ V : T A} \qquad \frac{M : T A \quad F : A \to T B}{M \star F : T B}$$

The untyped computational core λ_c (dLT 2020)

Given a monad T, consider the **call-by-value reflexive object** (Moggi 1988)

$$D = D \to TD$$

relating the types D and TD; hence we have two kinds of terms

$$\begin{array}{rcll} Val: & V, W & ::= & x \mid \lambda x.M \\ Com: & M, N & ::= & [V] \mid M \star V \end{array}$$

writing $[V] \equiv \mathit{unit}\ V$, with typing rules

$$\frac{}{\Gamma, x : D \vdash x : D} \qquad \frac{\Gamma, x : D \vdash M : TD}{\Gamma \vdash \lambda x.M : D \to TD = D}$$

$$\frac{\Gamma \vdash V : D}{\Gamma \vdash [V] : TD} \qquad \frac{\Gamma \vdash M : TD \qquad \Gamma \vdash V : D = D \to TD}{\Gamma \vdash M \star V : TD}$$

The untyped computational core λ_c (dLT 2020)

Given a monad T, consider the **call-by-value reflexive object** (Moggi 1988)

$$D = D \to TD$$

relating the types D and TD; hence we have two kinds of terms

$$\begin{array}{llll} Val: & V, W & ::= & x \mid \lambda x.M \\ Com: & M, N & ::= & [V] \mid M \star V \end{array}$$

writing $[V] \equiv \mathit{unit}\ V$, with interpretation maps

$$[\![\cdot]\!]^{D} : Val \to Env \to D \qquad [\![\cdot]\!]^{TD} : Com \to Env \to TD$$

$$\begin{array}{ll} [\![x]\!]^{D} e = e(x) & [\![\lambda x.M]\!]^{D} e = \Psi(\lambda\!\!\lambda\, d \in D.\, [\![M]\!]^{TD} e[x \mapsto d]) \\ [\![\, [V] \,]\!]^{TD} e = \mathit{unit}\ ([\![V]\!]^{D} e) & [\![M \star V]\!]^{TD} e = ([\![M]\!]^{TD} e) \star \Phi([\![V]\!]^{D} e) \end{array}$$

where $e \in Env = Var \to D$, $\Phi : D \xrightarrow{\sim} [D \to TD]$ and $\Psi = \Phi^{-1}$

The partiality and state monad $\mathbb{S}$ over **Dom**

Set $\mathbb{L} = \{\ell_0, \ell_1, \ldots\}$ **locations** and $Y \in$ **Dom**

$$S = Y^{\mathbb{L}} = [\mathbb{L} \to Y] \text{ domain of } \textbf{states}$$

The **partiality and state monad** is the triple $(\mathbb{S}, \mathit{unit}, \star)$:

$$\mathbb{S}\, X = S \to (X \times S)_\perp$$

equipped with two (families of) operators *unit* and $\star$:

$$\mathit{unit}\, x\, \varsigma = (x, \varsigma) \qquad (c \star f)\, \varsigma = \begin{cases} f\,(x)(\varsigma') & \text{if } c(\varsigma) = (x, \varsigma') \neq \perp \\ \perp & \text{if } c(\varsigma) = \perp \end{cases}$$

for $c \in \mathbb{S}X$ and $\varsigma \in S$

A domain equation

Theorem

There exists a domain $D \in \mathrm{Dom}$ *solving the equation*

$$D = D \to S \to (D \times S)_{\perp}$$

where $S = \mathbb{L} \to D$. *If* $\mathbb{S}$ *is the monad with states in* S *then* D *solves*

$$D = D \to \mathbb{S}\, D$$

Algebraic operators à la Plotkin and Power

Algebraic operators are morphisms $\mathbf{op}_X : (TX)^n \to TX$ s.t.

$$\mathbf{op}_X \circ (\underbrace{f^\dagger \times \cdots \times f^\dagger}_{n}) = f^\dagger \circ \mathbf{op}_X \quad \text{with } f : X \to TX$$

Algebraic operators à la Plotkin and Power

Algebraic operators are morphisms $\mathbf{op}_X : (TX)^n \to TX$ s.t.

$$\mathbf{op}_X \circ (\underbrace{f^\dagger \times \cdots \times f^\dagger}_{n}) = f^\dagger \circ \mathbf{op}_X \quad \text{with } f : X \to TX$$

In general, if A is a domain of **abstract arities** and P of **parameters** then

$$\mathbf{op} : P \times (TX)^A \to TX \cong (TX)^A \to (TX)^P$$

$$\mathbf{op}(p, k) \star f = f^\dagger(\mathbf{op}(p, k)) = \mathbf{op}(p, f^\dagger \circ k) = \mathbf{op}(p, \lambda\!\!\lambda x.(k(x) \star f))$$

Algebraic operators à la Plotkin and Power

Algebraic operators are morphisms $\mathbf{op}_X : (TX)^n \to TX$ s.t.

$$\mathbf{op}_X \circ (\underbrace{f^\dagger \times \cdots \times f^\dagger}_{n}) = f^\dagger \circ \mathbf{op}_X \quad \text{with } f : X \to TX$$

In general, if A is a domain of **abstract arities** and P of **parameters** then

$$\mathbf{op} : P \times (TX)^A \to TX \cong (TX)^A \to (TX)^P$$

$$\mathbf{op}(p,k) \star f = f^\dagger(\mathbf{op}(p,k)) = \mathbf{op}(p, f^\dagger \circ k) = \mathbf{op}(p, \lambda\!\!\lambda x.(k(x) \star f))$$

Example

In case of $T = \mathbb{S}$, taking $P = \mathbf{1}$ and $A = D$ we define:

$$\mathbf{get}_\ell : \mathbf{1} \times (\mathbb{S}D)^D \to \mathbb{S}D \simeq D \to \mathbb{S}D \quad \text{by} \quad \mathbf{get}_\ell\, d\, \varsigma = d\,(\varsigma\,(\ell))\,\varsigma$$

Taking $P = D$ and $A = \mathbf{1}$, we define:

$$\mathbf{set}_\ell : D \times (\mathbb{S}D)^{\mathbf{1}} \to \mathbb{S}D \simeq D \times \mathbb{S}D \to \mathbb{S}D \quad \text{by} \quad \mathbf{set}_\ell(d,c)\,\varsigma = c(\varsigma[\ell \mapsto d])$$

The imperative calculus λ_{imp}

Syntax

$$\begin{array}{llll} Val: & V, W & ::= & x \mid \lambda x.M \\ Com: & M, N & ::= & [V] \mid M \star V \mid get_\ell(\lambda x.M) \mid set_\ell(V, M) \qquad (\ell \in \mathbb{L}) \end{array}$$

Semantics

$$[\![\cdot]\!]^D : Val \to Env \to D \qquad [\![\cdot]\!]^{\mathbb{S}D} : Com \to Env \to \mathbb{S}D$$

$$\begin{array}{ll} [\![x]\!]^D e = e(x) & [\![\lambda x.M]\!]^D e = \Psi(\lambda\!\!\lambda\, d \in D.\, [\![M]\!]^{\mathbb{S}D} e[x \mapsto d]) \\ [\![\,[V]\,]\!]^{\mathbb{S}D} e = unit\ ([\![V]\!]^D e) & [\![M \star V]\!]^{\mathbb{S}D} e = ([\![M]\!]^{\mathbb{S}D} e) \star \Phi([\![V]\!]^D e) \end{array}$$

$$[\![get_\ell(\lambda x.M)]\!]^{\mathbb{S}D} e = \mathbf{get}_\ell\, \Phi([\![\lambda x.M]\!]^D e)$$
$$[\![set_\ell(V, M)]\!]^{\mathbb{S}D} e = \mathbf{set}_\ell([\![V]\!]^D e, [\![M]\!]^{\mathbb{S}D} e)$$

where $Env = Var \to D$, $\Phi : D \xrightarrow{\sim} [D \to \mathbb{S}D]$ and $\Psi = \Phi^{-1}$

Types as (duals of) compact points

In ω-**ALG**, the full subcategory of **Dom** of algebraic lattices with countable basis, we have

$$D \cong \mathcal{I}(\mathcal{K}(D)) \cong \mathcal{F}(\mathcal{K}^{op}(D)) \qquad \text{for any } D \in \omega\text{-}\mathbf{ALG}$$

Types as (duals of) compact points

In ω-**ALG**, the full subcategory of **Dom** of algebraic lattices with countable basis, we have

$$D \cong \mathcal{I}(\mathcal{K}(D)) \cong \mathcal{F}(\mathcal{K}^{op}(D)) \qquad \text{for any } D \in \omega\text{-}\mathbf{ALG}$$

An **intersection type theory** $Th = (\mathcal{L}, \leqslant)$ is a *finitary* presentation of $\mathcal{K}^{op}(D)$ s.t.

$$\mathcal{K}(D) \ni d \leftarrow\!\!\mid \sigma_d \in \mathcal{L}_D \qquad \text{and} \qquad d \sqsubseteq e \iff \sigma_e \leqslant_D \sigma_d$$

Types as (duals of) compact points

In ω-**ALG**, the full subcategory of **Dom** of algebraic lattices with countable basis, we have

$$D \cong \mathcal{I}(\mathcal{K}(D)) \cong \mathcal{F}(\mathcal{K}^{op}(D)) \qquad \text{for any } D \in \omega\text{-}\mathbf{ALG}$$

An **intersection type theory** $Th = (\mathcal{L}, \leqslant)$ is a *finitary* presentation of $\mathcal{K}^{op}(D)$ s.t.

$$\mathcal{K}(D) \ni d \leftarrow\!\!\!\dashv \sigma_d \in \mathcal{L}_D \qquad \text{and} \qquad d \sqsubseteq e \iff \sigma_e \leqslant_D \sigma_d$$

$$[\![M]\!]^D \quad = \quad \bigsqcup\{d \in \mathcal{K}(D) \mid d \sqsubseteq [\![M]\!]^D\} \quad = \quad \bigsqcup \mathcal{K}([\![M]\!]^D)$$

$$\begin{aligned}
d \sqsubseteq [\![M]\!]^D \quad &\iff \quad \downarrow d \subseteq \mathcal{K}([\![M]\!]^D) \\
&\iff \quad [\![M]\!]^{\mathcal{F}} \supseteq \uparrow \sigma_d \\
&\iff \quad [\![M]\!]^{\mathcal{F}} \ni \sigma_d \\
&\iff \quad \vdash M : \sigma_d
\end{aligned}$$

The filter model $\mathcal{F}_D \cong [\mathcal{F}_D \to \mathbb{S}\mathcal{F}_D]$ of λ_{imp}

Theorem

There are theories Th_D and $Th_{\mathbb{S}D}$ such that $\mathcal{F}_D = \mathcal{F}_{D \to \mathbb{S}D} \cong [\mathcal{F}_D \to \mathbb{S}\mathcal{F}_D]$

Proof. By defining the theories Th_D, Th_S, Th_C with $C = (D \times S)_\perp$, and $Th_{\mathbb{S}D}$ by mutual induction:

$$\begin{array}{llll} \mathcal{L}_D : & \delta & ::= & \delta \to \tau \mid \delta \wedge \delta' \mid \omega_D \\ \mathcal{L}_C : & \kappa & ::= & \delta \times \sigma \mid \kappa \wedge \kappa' \mid \omega_C \end{array} \qquad \begin{array}{llll} \mathcal{L}_S : & \sigma & ::= & \langle \ell : \delta \rangle \mid \sigma \wedge \sigma' \mid \omega_S \\ \mathcal{L}_{\mathbb{S}D} : & \tau & ::= & \sigma \to \kappa \mid \tau \wedge \tau' \mid \omega_{\mathbb{S}D} \end{array}$$

plus axioms and rules e.g.

$$(\sigma \to \kappa) \wedge (\sigma \to \kappa') \leqslant_{\mathbb{S}D} \sigma \to \kappa \wedge \kappa' \qquad \frac{\sigma' \leqslant_S \sigma \quad \kappa \leqslant_C \kappa'}{\sigma \to \kappa \leqslant_{\mathbb{S}D} \sigma' \to \kappa'}$$

The interpretations $[\![V]\!]^{\mathcal{F}_D}$ and $[\![M]\!]^{\mathcal{F}_{\mathbb{S}D}}$

From the definition of $\star$ in case of $\mathbb{S}$ we get

$$[\![M \star V]\!]^{\mathcal{F}_{\mathbb{S}D}} e = ([\![M]\!]^{\mathcal{F}_{\mathbb{S}D}} e) \star^{\mathcal{F}} ([\![V]\!]^{\mathcal{F}_D} e)$$

The interpretations $[\![V]\!]^{\mathcal{F}_D}$ and $[\![M]\!]^{\mathcal{F}_{\mathbb{S}D}}$

From the definition of $\star$ in case of $\mathbb{S}$ we get

$$[\![M \star V]\!]^{\mathcal{F}_{\mathbb{S}D}} e = ([\![M]\!]^{\mathcal{F}_{\mathbb{S}D}} e) \star^{\mathcal{F}} ([\![V]\!]^{\mathcal{F}_D} e)$$

Defining (after BCD'83)

$$X \cdot Y = \{\psi \mid \exists \varphi \in Y.\, \varphi \to \psi \in X\}$$

for $X \in \mathcal{F}_{\mathbb{S}D}$, $Y \in \mathcal{F}_D$ and $Z \in \mathcal{F}_S$ we have

$$(X \star^{\mathcal{F}} Y) \cdot Z = \begin{cases} (Y \cdot U) \cdot V & \text{if } X \cdot Z = U \times V \neq {\uparrow_C}\, \omega_C \\ {\uparrow_C}\, \omega_C & \text{otherwise} \end{cases}$$

then we conclude that

$$\begin{array}{rcl} [\![M \star V]\!]^{\mathcal{F}_{\mathbb{S}D}} e & = & \mathtt{Filt}\{\ \sigma \to \delta'' \times \sigma'' \in \mathcal{L}_{\mathbb{S}D} \mid \\ & & \quad \exists \delta', \sigma'.\, \sigma \to \delta' \times \sigma' \in [\![M]\!]^{\mathcal{F}_{\mathbb{S}D}} e \ \ \& \\ & & \qquad \delta' \to \sigma' \to \delta'' \times \sigma'' \in [\![V]\!]^{\mathcal{F}_D} e\} \end{array}$$

where $\mathtt{Filt}\, X$ is the least filter including X.

From interpretations to typing rules

To $\Gamma = \{x_1 : \delta_1, \ldots, x_n : \delta_n\}$ we associate the environment $e_\Gamma : Var \rightarrow \mathcal{F}_D$

$$e_\Gamma(x) = \begin{cases} \uparrow_D \delta & \text{if } x : \delta \in \Gamma \\ \uparrow_D \omega_D & \text{otherwise} \end{cases}$$

Then from the semantics of $Q \equiv op(P_1, \ldots, P_n)$ we have

$$[\![Q]\!]^{\mathcal{F}} e_\Gamma = \mathtt{Filt}\{\psi \mid \varphi_1 \in [\![P_1]\!]^{\mathcal{F}} e_{\Gamma_1} \ \& \ \cdots \ \& \ \varphi_n \in [\![P_n]\!]^{\mathcal{F}} e_{\Gamma_n}\}$$

From interpretations to typing rules

Factoring out the $\texttt{Filt}\{\cdots\}$ operator by the rules

$$\frac{}{\Gamma \vdash P : \omega}\,(\omega) \qquad \frac{\Gamma \vdash P : \varphi \quad \Gamma \vdash P : \psi}{\Gamma \vdash P : \varphi \wedge \psi}\,(\wedge) \qquad \frac{\Gamma \vdash P : \varphi \quad \varphi \leqslant \psi}{\Gamma \vdash P : \psi}\,(\leqslant)$$

it suffices to guarantee

$$[\![Q]\!]^{\mathcal{F}} e_{\Gamma} \supseteq \{\psi \mid \varphi_1 \in [\![P_1]\!]^{\mathcal{F}} e_{\Gamma_1} \ \& \ \cdots \ \& \ \varphi_n \in [\![P_n]\!]^{\mathcal{F}} e_{\Gamma_n}\}$$

which is obtained by the rule

$$\frac{\Gamma_1 \vdash P_1 : \varphi_1 \quad \cdots \quad \Gamma_n \vdash P_n : \varphi_n}{\Gamma \vdash Q : \psi}$$

Example

From

$$\begin{array}{rcl} [\![M \star V]\!]^{\mathcal{F}_{\mathbb{S}D}} e_\Gamma & = & ([\![M]\!]^{\mathcal{F}_{\mathbb{S}D}} e_\Gamma) \star^{\mathcal{F}} ([\![V]\!]^{\mathcal{F}_D} e_\Gamma) \\ & = & \mathtt{Filt}\{\sigma \to \delta'' \times \sigma'' \in \mathcal{L}_{\mathbb{S}D} \mid \\ & & \exists \delta', \sigma'.\ \sigma \to \delta' \times \sigma' \in [\![M]\!]^{\mathcal{F}_{\mathbb{S}D}} e_\Gamma \ \ \& \\ & & \delta' \to \sigma' \to \delta'' \times \sigma'' \in [\![V]\!]^{\mathcal{F}_D} e_\Gamma \} \end{array}$$

we get the rule

$$\frac{\Gamma \vdash M : \sigma \to \delta' \times \sigma' \quad \Gamma \vdash V : \delta' \to \sigma' \to \delta'' \times \sigma''}{\Gamma \vdash M \star V : \sigma \to \delta'' \times \sigma''} \ (\star)$$

The type assignment system

Rewriting as rules the clauses in the definition of $[\![V]\!]^{\mathcal{F}_D}$ and $[\![M]\!]^{\mathcal{F}_{\mathbb{S}D}}$, we obtain

$$\frac{}{\Gamma, x : \delta \vdash x : \delta}\ (var) \qquad \frac{\Gamma, x : \delta \vdash M : \tau}{\Gamma \vdash \lambda x.M : \delta \to \tau}\ (\lambda)$$

$$\frac{\Gamma \vdash V : \delta}{\Gamma \vdash [V] : \sigma \to \delta \times \sigma}\ (unit) \qquad \frac{\Gamma \vdash M : \sigma \to \delta' \times \sigma' \quad \Gamma \vdash V : \delta' \to \sigma' \to \delta'' \times \sigma''}{\Gamma \vdash M \star V : \sigma \to \delta'' \times \sigma''}\ (\star)$$

$$\frac{\Gamma, x : \delta \vdash M : \sigma \to \kappa}{\Gamma \vdash get_\ell(\lambda x.M) : (\langle \ell : \delta \rangle \wedge \sigma) \to \kappa}\ (get) \qquad \frac{\Gamma \vdash V : \delta \quad \Gamma \vdash M : (\langle \ell : \delta \rangle \wedge \sigma) \to \kappa \quad \ell \notin dom(\sigma)}{\Gamma \vdash set_\ell(V, M) : \sigma \to \kappa}\ (set)$$

$$\frac{}{\Gamma \vdash P : \omega}\ (\omega) \qquad \frac{\Gamma \vdash P : \varphi \quad \Gamma \vdash P : \psi}{\Gamma \vdash P : \varphi \wedge \psi}\ (\wedge) \qquad \frac{\Gamma \vdash P : \varphi \quad \varphi \leqslant \psi}{\Gamma \vdash P : \psi}\ (\leqslant)$$

Results

Results

For $A = D, S, (D \times S)_\perp$, and $\mathbb{S}D$, and $\varphi \in \mathcal{L}_A$ define:

$$[\![\varphi]\!]^{\mathcal{F}} = \{X \in \mathcal{F}_A \mid \varphi \in X\}$$

Theorem (Type Semantics)

Let $e \models^{\mathcal{F}} \Gamma$ *if and only if* $e(x) \in [\![\delta]\!]^{\mathcal{F}}$ *whenever* $x : \delta \in \Gamma$*; then*

1. $[\![V]\!]^{\mathcal{F}_D} e = \{\delta \in \mathcal{L}_D \mid \exists \Gamma.\ e \models^{\mathcal{F}} \Gamma \ \&\ \Gamma \vdash V : \delta\}$
2. $[\![M]\!]^{\mathcal{F}_{\mathbb{S}D}} e = \{\tau \in \mathcal{L}_{\mathbb{S}D} \mid \exists \Gamma.\ e \models^{\mathcal{F}} \Gamma \ \&\ \Gamma \vdash M : \tau\}$

Results

For $A = D, S, (D \times S)_\perp$, and $\mathbb{S}D$, and $\varphi \in \mathcal{L}_A$ define:

$$[\![\varphi]\!]^{\mathcal{F}} = \{X \in \mathcal{F}_A \mid \varphi \in X\}$$

Theorem (Type Semantics)

Let $e \models^{\mathcal{F}} \Gamma$ if and only if $e(x) \in [\![\delta]\!]^{\mathcal{F}}$ whenever $x : \delta \in \Gamma$; then

1. $[\![V]\!]^{\mathcal{F}_D} e = \{\delta \in \mathcal{L}_D \mid \exists \Gamma .\ e \models^{\mathcal{F}} \Gamma \ \&\ \Gamma \vdash V : \delta\}$
2. $[\![M]\!]^{\mathcal{F}_{\mathbb{S}D}} e = \{\tau \in \mathcal{L}_{\mathbb{S}D} \mid \exists \Gamma .\ e \models^{\mathcal{F}} \Gamma \ \&\ \Gamma \vdash M : \tau\}$

For $D \cong D \to \mathbb{S}D$, $P \in Val \cup Com$, $\varphi \in \mathcal{L}_D \cup \mathcal{L}_{\mathbb{S}D}$ define

$$\Gamma \models^D P : \varphi \iff \forall e \in Env.\ e \models^D \Gamma \Longrightarrow [\![P]\!]^D e \in [\![\varphi]\!]^D$$

and let $\Gamma \models P : \varphi$ if and only if $\Gamma \models^D P : \varphi$ for all D modeling λ_{imp}

Corollary (Soundness and Completeness)

For all $V \in Val$ and $\delta \in \mathcal{L}_D$, and for all $M \in Com$ and $\tau \in \mathcal{L}_{\mathbb{S}D}$

$$\Gamma \vdash V : \delta \iff \Gamma \models V : \delta \quad \text{and} \quad \Gamma \vdash M : \tau \iff \Gamma \models M : \tau .$$

Future work

We have described a **particular case** of **a general pattern**

Next steps could be

- to describe categorically the method followed here
- to consider a generic monad T *and* **generic algebraic operators** over T
- to consider **other categories** than ω-**ALG**, such as coherent spaces, event structures, and **Rel**