CPSC 429/529: Functional Programming
Carsten Schürmann
Date: February 11, 2001

Lecture 12: Type preservation

1 Syntactic Categories

Types:	τ	$::=$	$\tau_1 \to \tau_2 \mid [\tau]$
Environments:	E	$::=$	$\cdot \mid E, x = C$
Closures:	C	$::=$	$\{E; P\}$
Values:	V	$::=$	$\lambda x : \tau . P \mid [] \mid P_1 : P_2$
Programs:	P	$::=$	$V \mid x \mid P_1\ P_2$
			$\mid (\text{case } P \text{ of } [] \to P_1 \mid (h : t) \to P_2) \mid \mu x : \tau . P$
Contexts:	Γ	$::=$	$\cdot \mid \Gamma, x : \tau$

2 Evaluation

Definition 2.1 (Evaluating programs) $E \vdash P \hookrightarrow C$

$$\frac{}{E \vdash V \hookrightarrow \{E; V\}}\ \textsf{evval} \qquad \frac{E(x) = \{E'; P'\} \qquad E' \vdash P' \hookrightarrow C}{E \vdash x \hookrightarrow C}\ \textsf{evvar}$$

$$\frac{E \vdash P_1 \hookrightarrow \{E'; \lambda x : \tau . P_1'\} \qquad E', \{E; P_2\} \vdash P_1' \hookrightarrow C}{E \vdash P_1 P_2 \hookrightarrow C}\ \textsf{evapp}$$

$$\frac{E \vdash P \hookrightarrow [] \qquad E \vdash P_1 \hookrightarrow C}{E \vdash \begin{pmatrix} \textit{case } P \\ \quad \textit{of } [] \to P_1 \\ \quad \mid \ (h : t) \to P_2 \end{pmatrix} \hookrightarrow C}\ \textsf{evcasenil}$$

$$\frac{E \vdash P \hookrightarrow \{E'; (P_h : P_t)\} \qquad E, h = \{E'; P_h\}, t = \{E'; P_t\} \vdash P_2 \hookrightarrow C}{E \vdash \begin{pmatrix} \textit{case } P \\ \quad \textit{of } [] \to P_1 \\ \quad \mid \ (h : t) \to P_2 \end{pmatrix} \hookrightarrow C}\ \textsf{evcasecons}$$

$$\frac{E, \{E; \mu x : \tau . P\} \vdash P \hookrightarrow C}{E \vdash \mu x : \tau . P \hookrightarrow C}\ \textsf{evfix}$$

3 Typing rules

Definition 3.1 (Valid Values and Programs) $\Gamma \vdash V : \tau$, $\Gamma \vdash P : \tau$

$$\frac{\Gamma, x : \tau_1 \vdash P : \tau_2}{\Gamma \vdash \lambda x : \tau_1 . P : \tau_1 \to \tau_2}\,\mathsf{oflam} \qquad \frac{}{\Gamma \vdash [] : [\tau]}\,\mathsf{ofnil} \qquad \frac{\Gamma \vdash P_1 : \tau \qquad \Gamma \vdash P_2 : [\tau]}{\Gamma \vdash (P_1 : P_2) : [\tau]}\,\mathsf{ofcons}$$

$$\frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau}\,\mathsf{ofvar} \qquad \frac{\Gamma \vdash P : [\tau] \qquad \Gamma \vdash P_1 : \tau' \qquad \Gamma, h : \tau, t : [\tau] \vdash P_2 : \tau'}{\Gamma \vdash \begin{pmatrix} \mathit{case}\ P & \\ \quad \mathit{of}\ [] \to P_1 & \\ \quad \mid \quad (h : t) \to P_2 & \end{pmatrix} : \tau'}\,\mathsf{oflist}$$

$$\frac{\Gamma, x : \tau \vdash P : \tau}{\Gamma \vdash \mu x : \tau . P : \tau}\,\mathsf{offix}$$

Definition 3.2 (Valid Environments) $\vdash E : \Gamma$

$$\frac{}{\vdash \cdot : \cdot}\,\mathsf{ofEnil} \qquad \frac{\vdash E : \Gamma \qquad \Gamma \vdash C : \tau}{\vdash E : x = C : \Gamma, x : \tau}\,\mathsf{ofEcons}$$

Definition 3.3 (Valid Closures) $\Gamma \vdash C : \tau$

$$\frac{\vdash E : \Gamma \qquad \Gamma \vdash P : \tau}{\vdash \{E; P\} : \tau}\,\mathsf{ofclo}$$

4 Some properties of Mini-Haskell

Theorem 4.1 (Value soundness) *Let E be an environment, P a program, and C a closure. If*

$$\begin{array}{c}\mathcal{D}\\ E \vdash P \hookrightarrow C\end{array}$$

then $C = \{E'; V'\}$ where E' is an environment, and V' a value.

Proof: by induction on $\mathcal{D}$.

Case: $\mathcal{D} = \dfrac{}{E \vdash V \hookrightarrow \{E; V\}}\,\mathsf{evval}$. Clear.

Case: $\mathcal{D} = \dfrac{E(x) = \{E'; P'\} \qquad \begin{array}{c}\mathcal{D}'\\ E' \vdash P' \hookrightarrow C\end{array}}{E \vdash x \hookrightarrow C}\,\mathsf{evvar}$.

$C = \{E'; V'\}$ by induction hypothesis on $\mathcal{D}'$.

All other cases by application of the induction hypothesis. $\square$

Theorem 4.2 (Type preservation) *Let E be an environment, P a program, C a closure, Γ a context and τ a type.*

$$\text{If}\quad \overset{\mathcal{D}}{E \vdash P \hookrightarrow C} \quad\text{and}\quad \overset{\mathcal{E}}{\vdash E : \Gamma} \quad\text{and}\quad \overset{\mathcal{P}}{\Gamma \vdash P : \tau} \quad\text{then}\quad \overset{\mathcal{Q}}{\vdash C : \tau}\ .$$

Proof: by induction on $\mathcal{D}$.

Case: $\mathcal{D} = \dfrac{}{E \vdash V \hookrightarrow \{E; V\}}\,\mathsf{evval}.$

$\vdash \{E; V\} : \tau$	by ofclo on $\mathcal{E}$, $\mathcal{P}$

Case: $\mathcal{D} = \dfrac{E(x) = \{E'; P'\} \qquad \overset{\mathcal{D}'}{E' \vdash P' \hookrightarrow C}}{E \vdash x \hookrightarrow C}\,\mathsf{evvar}.$

$\mathcal{Q}_1 :: \vdash \{E'; P'\} : \tau$	by lookup of x in E
$\mathcal{E}_1 :: \vdash E' : \Gamma'$	by inversion on $\mathcal{Q}_1$ using ofclo
$\mathcal{P}_1 :: \Gamma' \vdash P' : \tau$	by inversion on $\mathcal{Q}_1$ using ofclo
$\mathcal{Q}_2 :: \vdash C : \tau$	by induction hypothesis on $\mathcal{D}'$, $\mathcal{E}_1$, and $\mathcal{P}_1$

Case: $\mathcal{D} = \dfrac{\overset{\mathcal{D}_1}{E \vdash P_1 \hookrightarrow \{E'; \lambda x : \tau .\, P_1'\}} \qquad \overset{\mathcal{D}_2}{E', \{E; P_2\} \vdash P_1' \hookrightarrow C}}{E \vdash P_1\ P_2 \hookrightarrow C}\,\mathsf{evapp}.$

$\mathcal{P}_1 :: \Gamma \vdash P_1 : \tau_2 \to \tau$	by inversion on $\mathcal{P}$ using ofapp
$\mathcal{P}_2 :: \Gamma \vdash P_2 : \tau_2$	by inversion on $\mathcal{P}$ using ofapp
$\mathcal{Q}_1 :: \vdash \{E'; \lambda x : \tau_2 .\, P_1'\} : \tau_2 \to \tau$	by induction hypothesis on $\mathcal{D}_1$, $\mathcal{E}$, $\mathcal{P}_1$
$\mathcal{E}_1 :: \vdash E' : \Gamma'$	by inversion using ofclo
$\mathcal{P}_3 :: \Gamma' \vdash \lambda x : \tau_2 .\, P_1' : \tau_2 \to \tau$	by inversion using ofclo
$\mathcal{P}_4 :: \Gamma', x : \tau_2 \vdash P_1' : \tau$	by inversion using oflam on $\mathcal{P}_3$
$\mathcal{Q}_2 :: \vdash \{E; P_2\} : \tau_2$	by ofclo on $\mathcal{E}$, $\mathcal{P}_2$
$\mathcal{E}_2 :: \vdash E', x = \{E; P_2\} : \Gamma', x : \tau_2$	by $\mathsf{ofEcons}$ on $\mathcal{E}_1$ and $\mathcal{Q}_1$
$\mathcal{Q}_3 :: \vdash C : \tau$	by induction hypothesis on $\mathcal{D}_2$, $\mathcal{E}_2$, and $\mathcal{P}_4$

Case: $\mathcal{D} = \dfrac{\overset{\mathcal{D}_1}{E \vdash P \hookrightarrow []} \qquad \overset{\mathcal{D}_2}{E \vdash P_1 \hookrightarrow C}}{E \vdash \begin{pmatrix} \text{case } P & & \\ \quad \text{of } [] \to P_1 & & \\ \quad\ \mid\ \ (h : t) \to P_2 & & \end{pmatrix} \hookrightarrow C}\,\mathsf{evcasenil}\ .$

$\mathcal{P}_1 :: \Gamma \vdash P_1 : \tau$ by inversion on $\mathcal{P}$ using ofapp
$\mathcal{Q}_1 :: \vdash C : \tau$ by induction hypothesis on $\mathcal{D}_1$, $\mathcal{E}$, $\mathcal{P}_1$

Case: $$\mathcal{D} = \dfrac{\begin{matrix}\mathcal{D}_1 \\ E \vdash P \hookrightarrow \{E'; (P_h : P_t)\}\end{matrix} \qquad \begin{matrix}\mathcal{D}_2 \\ E, h = \{E'; P_h\}, t = \{E'; P_t\} \vdash P_2 \hookrightarrow C\end{matrix}}{E \vdash \begin{pmatrix} \text{case } P \\ \quad \text{of } [] \to P_1 \\ \quad \mid \ (h : t) \to P_2 \end{pmatrix} \hookrightarrow C} \textsf{evcasecons}.$$

$\mathcal{P}_1 :: \Gamma \vdash P : [\tau_1]$ by inversion on $\mathcal{P}$ using ofapp
$\mathcal{P}_2 :: \Gamma, h : \tau_1, t : [\tau_1] \vdash P_2 : \tau$ by inversion on $\mathcal{P}$ using ofapp
$\mathcal{Q}_1 :: \vdash \{E'; (P_h : P_t)\} : [\tau_1]$ by induction hypothesis on $\mathcal{D}_1$, $\mathcal{E}$, $\mathcal{P}_1$
$\mathcal{E}_1 :: \vdash E' : \Gamma'$ by inversion on $\mathcal{Q}_1$ using ofclo
$\mathcal{P}_3 :: \Gamma' \vdash (P_h : P_t) : [\tau_1]$ by inversion on $\mathcal{Q}_1$ using ofclo
$\mathcal{P}_4 :: \Gamma' \vdash P_h : \tau_1$ by inversion on $\mathcal{P}_3$ using ofcons
$\mathcal{P}_5 :: \Gamma' \vdash P_t : [\tau_1]$ by inversion on $\mathcal{P}_3$ using ofcons
$\mathcal{Q}_2 :: \vdash \{E'; P_h\} : \tau_1$ by ofclo on $\mathcal{E}_1$, $\mathcal{P}_4$
$\mathcal{Q}_3 :: \vdash \{E'; P_t\} : [\tau_1]$ by ofclo on $\mathcal{E}_1$, $\mathcal{P}_5$
$\mathcal{E}_2 :: \vdash E, h = \{E'; P_h\} : \Gamma, h : \tau_1$ by ofEcons on $\mathcal{E}_1$ and $\mathcal{Q}_2$
$\mathcal{E}_3 :: \vdash E, h = \{E'; P_h\}, t = \{E'; P_t\} : \Gamma, h : \tau_1, t : [\tau_1]$
by ofEcons on $\mathcal{E}_2$ and $\mathcal{Q}_3$
$\mathcal{Q}_4 :: \vdash C : \tau$ by induction hypothesis on $\mathcal{D}_2$, $\mathcal{E}_3$, $\mathcal{P}_2$

Case: $$\mathcal{D} = \dfrac{\begin{matrix}\mathcal{D}' \\ E, \{E; \mu x : \tau. P\} \vdash P \hookrightarrow C\end{matrix}}{E \vdash \mu x : \tau. P \hookrightarrow C} \textsf{evfix}.$$

$\mathcal{P}_1 :: \Gamma, x : \tau \vdash P : \tau$ by inversion on $\mathcal{P}$ using offix
$\mathcal{Q}_1 :: \vdash \{E; \mu x : \tau. P\} : \tau$ by ofclo on $\mathcal{E}$, $\mathcal{P}$
$\mathcal{E}_1 :: \vdash E, x = \{E; \mu x : \tau. P\} : \Gamma, x : \tau$ by ofEcons on $\mathcal{E}$ and $\mathcal{Q}_1$
$\mathcal{Q}_2 :: \vdash C : \tau$ by induction hypothesis on $\mathcal{D}'$, $\mathcal{E}_1$, $\mathcal{P}_1$

□