Universitetet i Oslo
Institutt for Informatikk
Reliable Systems
Martin Steffen

IN [5/9]440: static analysis

Autumn 2018

Handout 3

18. 9. 2018

Handout 3: Introduction: Type and effect systems

Issued: 18. 9. 2018

$$\vdash [x := a]^l : \Sigma \to \Sigma \quad \textsc{Ass}$$

$$[\mathsf{skip}]^l : \Sigma \to \Sigma \quad \textsc{Skip}$$

$$\frac{\vdash S_1 : \Sigma \to \Sigma \qquad S_2 : \Sigma \to \Sigma}{\vdash S_1; S_2 : \Sigma \to \Sigma}\ \textsc{Seq}$$

$$\frac{\vdash S : \Sigma \to \Sigma}{\vdash \mathtt{while}[b]^l\ \mathtt{do}\ S : \Sigma \to \Sigma}\ \textsc{While}$$

$$\frac{\vdash S_1 : \Sigma \to \Sigma \qquad \vdash S_2 : \Sigma \to \Sigma}{\vdash \mathtt{if}[b]^l\ \mathtt{then}\ S_1\ \mathtt{else}\ S_2 : \Sigma \to \Sigma}\ \textsc{Cond}$$

Figure 1: Trivial types system for while

$$\frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau}\ \textsc{Var}$$

$$\frac{\Gamma, x{:}\tau_1 \vdash e : \tau_2}{\Gamma \vdash\ \mathtt{fn}_\pi x \Rightarrow e : \tau_1 \to \tau_2}\ \textsc{Abs}$$

$$\frac{\Gamma \vdash e_1 : \tau_1 \to \tau_2 \qquad \Gamma \vdash e_2 : \tau_1}{\Gamma \vdash e_1\ e_2 : \tau_2}\ \textsc{App}$$

Figure 2: Simple type system

$$\frac{\hat{\Gamma}(x) = \hat{\tau}}{\hat{\Gamma} \vdash x : \hat{\tau} :: \emptyset}\ \textsc{Var}$$

$$\frac{\Gamma, x{:}\hat{\tau}_1 \vdash e : \hat{\tau}_2 :: \ \varphi}{\Gamma \vdash \texttt{fn}_\pi x \Rightarrow e : \hat{\tau}_1 \stackrel{\varphi \cup \{\pi\}}{\rightarrow} \hat{\tau}_2 :: \emptyset}\ \textsc{Abs}$$

$$\frac{\hat{\Gamma} \vdash e_1 : \hat{\tau}_1 \stackrel{\varphi}{\rightarrow} \hat{\tau}_2 :: \varphi_1 \qquad \hat{\Gamma} \vdash e_2 : \hat{\tau}_1 :: \varphi_2}{\hat{\Gamma} \vdash e_1\ e_2 : \hat{\tau}_2 :: \varphi \cup \varphi_1 \cup \varphi_2}\ \textsc{App}$$

Table 1: Call tracking

$$\vdash [x := a]^{l'} : \mathsf{RD} \rightarrow \mathsf{RD} \setminus \{(x,l) \mid l \in \mathbf{Lab}\} \cup \{(x,l')\} \qquad \textsc{ass}$$

$$\vdash [\mathsf{skip}]^{l} : \mathsf{RD} \rightarrow \mathsf{RD} \qquad \textsc{skip}$$

$$\frac{\vdash S_1 : \mathsf{RD}_1 \rightarrow \mathsf{RD}_2 \qquad \vdash S_2 : \mathsf{RD}_2 \rightarrow \mathsf{RD}_3}{\vdash S_1; S_2 : \mathsf{RD}_1 \rightarrow \mathsf{RD}_3}\ \textsc{Seq}$$

$$\frac{\vdash S_1 : \mathsf{RD}_1 \rightarrow \mathsf{RD}_2 \qquad \vdash S_2 : \mathsf{RD}_1 \rightarrow \mathsf{RD}_2}{\vdash \texttt{if}[b]^l\,\texttt{then}\,S_1\,\texttt{else}\,S_2 : \mathsf{RD}_1 \rightarrow \mathsf{RD}_2}\ \textsc{If}$$

$$\frac{\vdash S : \mathsf{RD} \rightarrow \mathsf{RD}}{\vdash \texttt{while}[b]^l\,\texttt{do}\,S : \mathsf{RD} \rightarrow \mathsf{RD}}\ \textsc{While}$$

$$\frac{\vdash S : \mathsf{RD}_1' \rightarrow \mathsf{RD}_2' \qquad \mathsf{RD}_1 \subseteq \mathsf{RD}_1' \qquad \mathsf{RD}_2' \subseteq \mathsf{RD}_2}{\vdash S : \mathsf{RD}_1 \rightarrow \mathsf{RD}_2}\ \textsc{Sub}$$

Table 2: Annotated base types

$$[x := a]^l : \Sigma \xrightarrow[\{(x,l)\}]{\{x\}} \Sigma \quad \text{Ass} \qquad [\mathsf{skip}]^l : \Sigma \xrightarrow[\emptyset]{\emptyset} \Sigma \quad \text{Skip}$$

$$\frac{S_1 : \Sigma \xrightarrow[\mathsf{RD}_1]{X_1} \Sigma \qquad S_2 : \Sigma \xrightarrow[\mathsf{RD}_2]{X_2} \Sigma}{S_1; S_2 : \Sigma \xrightarrow[\mathsf{RD}_1 \setminus X_2 \cup \mathsf{RD}_2]{X_1 \cup X_2} \Sigma} \text{Seq}$$

$$\frac{S_1 : \Sigma \xrightarrow[\mathsf{RD}]{X} \Sigma \qquad S_2 : \Sigma \xrightarrow[\mathsf{RD}]{X} \Sigma}{\mathtt{if}[b]^l\,\mathtt{then}\,S_1\,\mathtt{else}\,S_2 : \Sigma \xrightarrow[\mathsf{RD}]{X} \Sigma} \text{If}$$

$$\frac{S : \Sigma \xrightarrow[\mathsf{RD}]{X} \Sigma}{\mathtt{while}[b]^l\,\mathtt{do}\,S : \Sigma \xrightarrow[\mathsf{RD}]{\emptyset} \Sigma} \text{While}$$

$$\frac{S : \Sigma \xrightarrow[\mathsf{RD}']{X'} \Sigma \qquad X \subseteq X' \qquad \mathsf{RD}' \subseteq \mathsf{RD}}{S : \Sigma \xrightarrow[\mathsf{RD}]{X} \Sigma} \text{Sub}$$

Table 3: Annotated constr.

Exercise 1 Remember from the constraint solving part the analysis about CFA. The call-tracking analysis of today is rather similar. Try to formulate a CFA in the style of the call-tracking analyis.

Hint: The CFA can be formulated with judgments of the form

$$\Gamma \vdash e : \hat{\tau} \tag{1}$$

where the annotated types $\hat{\tau}$ are of the same form as in the call tracking analysis, i.e., function types are annotated as

$$\hat{\tau}_1 \xrightarrow{\varphi} \hat{\tau}_2 \tag{2}$$

$$\frac{?}{\Gamma \vdash X :?} \text{T-Var}$$

$$\frac{? \vdash ?}{\Gamma \vdash \underset{\pi}{\mathtt{fn}}\, X \Rightarrow e :?} \text{T-Abs}$$

$$\frac{? \vdash ? \qquad ? \vdash ?}{\Gamma \vdash e_1\ e_2 :?} \text{T-App}$$