Control-Flow Analysis (CFA) Handout

17-355/17-665/17-819: Program Analysis (Spring 2022)
Rohan Padhye

Functional Language

$$
\begin{array}{lcll}
e & \in & Expressions & \text{...or labelled terms} \\
t & \in & Term & \text{...or unlabelled expressions} \\
l & \in & \mathcal{L} & \text{labels}
\end{array}
$$

$$
\begin{array}{lcl}
e & ::= & t^l \\
t & ::= & \lambda x.e \\
 & | & x \\
 & | & (e_1)\ (e_2) \\
 & | & \text{let } x = e_1 \text{ in } e_2 \\
 & | & \text{if } e_0 \text{ then } e_1 \text{ else } e_2 \\
 & | & n \mid\ e_1 + e_2 \mid\ \ldots
\end{array}
$$

0-CFA Rules

$$\sigma \quad \in \quad \mathit{Var} \cup \mathit{Lab} \rightarrow L \qquad\qquad L \quad = \quad \mathbb{Z} + \top + \mathcal{P}(\lambda x.e)$$

$$\frac{}{[\![n]\!]^l \hookrightarrow \alpha(n) \sqsubseteq \sigma(l)}\ \mathit{const} \qquad \frac{[\![e_1]\!]^{l_1} \hookrightarrow C_1 \quad [\![e_2]\!]^{l_2} \hookrightarrow C_2}{[\![e_1^{l_1} + e_2^{l_2}]\!]^l \hookrightarrow C_1 \cup C_2 \cup (\sigma(l_1) +_\top \sigma(l_2)) \sqsubseteq \sigma(l)}\ \mathit{plus}$$

Where α is defined as we discussed in abstract interpretation, and $+_\top$ is addition lifted to work over a domain that includes $\top$ (and simply ignores/drops any lambda values). There are similar rules for other arithmetic operations.

$$\frac{}{[\![x]\!]^l \hookrightarrow \sigma(x) \sqsubseteq \sigma(l)}\ \mathit{var} \qquad \frac{[\![e]\!]^{l_0} \hookrightarrow C}{[\![\lambda x.e^{l_0}]\!]^l \hookrightarrow \{\lambda x.e\} \sqsubseteq \sigma(l) \cup C}\ \mathit{lambda}$$

$$\frac{[\![e_1]\!]^{l_1} \hookrightarrow C_1 \quad [\![e_2]\!]^{l_2} \hookrightarrow C_2}{[\![e_1^{l_1}\ e_2^{l_2}]\!]^l \hookrightarrow C_1 \cup C_2 \cup \textbf{fn}\ l_1 : l_2 \Rightarrow l}\ \mathit{apply}$$

$$\frac{\lambda x.e_0^{l_0} \in \sigma(l_1)}{\textbf{fn}\ l_1 : l_2 \Rightarrow l \hookrightarrow \sigma(l_2) \sqsubseteq \sigma(x) \wedge \sigma(l_0) \sqsubseteq \sigma(l)}\ \mathit{function\text{-}flow}$$

m-CFA Rules

$$\sigma \in (\mathit{Var} \cup \mathit{Lab}) \times \Delta \to L \qquad \Delta = \mathit{Lab}^{n \leqslant m} \qquad L = \mathbb{Z} + \top + \mathcal{P}((\lambda x.e, \delta))$$

$$\frac{}{\delta \vdash [\![n]\!]^l \hookrightarrow \alpha(n) \sqsubseteq \sigma(l, \delta)}\ \mathit{const}$$

$$\frac{}{\delta \vdash [\![x]\!]^l \hookrightarrow \sigma(x, \delta) \sqsubseteq \sigma(l, \delta)}\ \mathit{var}$$

$$\frac{}{\delta \vdash [\![\lambda x.e^{l_0}]\!]^l \hookrightarrow \{(\lambda x.e, \delta)\} \sqsubseteq \sigma(l, \delta)}\ \mathit{lambda}$$

$$\frac{\delta \vdash [\![e_1]\!]^{l_1} \hookrightarrow C_1 \qquad \delta \vdash [\![e_2]\!]^{l_2} \hookrightarrow C_2}{\delta \vdash [\![e_1^{l_1}\ e_2^{l_2}]\!]^l \hookrightarrow C_1 \cup C_2 \cup \mathbf{fn}_\delta\ l_1 : l_2 \Rightarrow l}\ \mathit{apply}$$

$$\frac{\begin{array}{c}(\lambda x.e_0^{l_0}, \delta) \in \sigma(l_1, \delta) \qquad \delta' = \mathit{suffix}(\delta{+}{+}l, m) \\ C_1 = \sigma(l_2, \delta) \sqsubseteq \sigma(x, \delta') \wedge \sigma(l_0, \delta') \sqsubseteq \sigma(l, \delta) \\ C_2 = \{\sigma(y, \delta) \sqsubseteq \sigma(y, \delta') \mid y \in FV(\lambda x.e_0)\} \\ \delta' \vdash [\![e_0]\!]^{l_0} \hookrightarrow C_3\end{array}}{\mathbf{fn}_\delta\ l_1 : l_2 \Rightarrow l \hookrightarrow C_1 \cup C_2 \cup C_3}\ \mathit{function\text{-}flow\text{-}}\delta$$