Information flow analysis

Language, Semantics

$$C \quad ::= \quad x := E \mid C_1 \,; C_2 \mid \mathbf{if}\ E\ \mathbf{then}\ C_1\ \mathbf{else}\ C_2 \mid \mathbf{while}\ E\ \mathbf{do}\ C$$

- For expressions, we assume there exists a semantic function $[\![E]\!] : \mathbf{Sto} \to \mathbf{Val}$ which satisfies the following property:

  If for all $x \in fv(E)$ we have $s_1\ x = s_2\ x$, with $s_1, s_2 \in \mathbf{Sto}$, then $[\![E]\!]s_1 = [\![E]\!]s_2$.

- The definition of $[\![E]\!]$ would contain the clause $[\![x]\!]s = s\ x$.
- The semantics of a command has functionality $[\![C]\!] : \mathbf{Trc} \to \mathbf{Trc}$.
- Because $\mathbf{Trc}$ is a CPO, therefore, with the following pointwise ordering, $\mathbf{Trc} \to \mathbf{Trc}$ is a CPO: $f_1 \sqsubseteq f_2$ iff $f_1(T) \sqsubseteq f_2(T)$ for all $T \in \mathbf{Trc}$.

Semantics, contd.

$$
\begin{aligned}
[\![x := E]\!] &= \lambda T.\lambda s.\text{let } s' = T\ s \text{ in } [s' \mid x \mapsto [\![E]\!]s'] \\
[\![C_1 \,; C_2]\!] &= \lambda T.[\![C_2]\!]([\![C_1]\!]T) \\
[\![\textbf{if } E \textbf{ then } C_1 \textbf{ else } C_2]\!] &= \lambda T.\lambda s.\text{let } s' = T\ s \text{ in} \\
&\quad \text{if } \textit{true?}([\![E]\!]s') \text{ then } [\![C_1]\!]T\ s \text{ else } [\![C_2]\!]T\ s \\
[\![\textbf{while } E \textbf{ do } C_0]\!] &= \mathit{lfp}(\mathcal{F}) \quad \text{where} \\
&\quad \mathcal{F} : (\mathbf{Trc} \to \mathbf{Trc}) \to (\mathbf{Trc} \to \mathbf{Trc}) \text{ is} \\
&\quad \mathcal{F}(f) = \lambda T.\lambda s.\text{let } s' = T\ s \text{ in} \\
&\quad \text{if } \textit{true?}([\![E]\!]s') \text{ then } f([\![C_0]\!]T)s \text{ else } s'
\end{aligned}
$$

Independences

- We will be interested in a finite abstraction of the pre-traces and the post-traces relevant to the execution of a command.
- The abstract traces are termed *independences*: an independence $\mathsf{T}^\# \in \textbf{Independ} = \mathcal{P}((\mathbf{Var} \cup \{\perp\}) \times \mathbf{Var})$ is a set of pairs of the form $[\mathtt{x} \ltimes w]$.
- If $\mathtt{x}$ is a variable, then $[\mathtt{x} \ltimes w]$ denotes that the *current* value of $\mathtt{x}$ is independent of the *initial* value of w.
- If $\mathtt{x}$ is $\perp$, then the *nontermination behavior* of the command is independent of w. This is formalized by the following definition of when an independence correctly describes a set of traces.

Definition of independences, ordering on independences

- For all $\mathsf{T} \in \mathbf{Trc}$, for all $x \in Var \cup \{\perp\}$, for all $w \in Var$, $\mathsf{T} \models [x \ltimes w]$ holds iff for all $s_1, s_2 \in \mathbf{Sto}_\perp$: $s_1 \underset{w}{=} s_2$ implies $\mathsf{T}\, s_1 \stackrel{x}{=} \mathsf{T}\, s_2$.

  $\mathsf{T} \models \mathsf{T}^\#$ holds iff for all $[x \ltimes w] \in \mathsf{T}^\#$ it holds that $\mathsf{T} \models [x \ltimes w]$.

- The ordering $\mathsf{T}_1^\# \preceq \mathsf{T}_2^\#$ holds iff $\mathsf{T}_2^\# \subseteq \mathsf{T}_1^\#$.

- **Independ** forms a complete lattice wrt. the ordering $\preceq$; let $\sqcap_i \mathsf{T}^\#{}_i$ denote the greatest lower bound (which is the set union).

Some facts

- If $T \models T_1^{\#}$ and $T_1^{\#} \preceq T_2^{\#}$ then $T \models T_2^{\#}$.
- If for all $i \in I$ it holds that $T \models T_i^{\#}$, then $T \models \sqcap_{i \in I} T_i^{\#}$.

Do we have an abstract interpretation?

- If $[x \ltimes w]$ belongs to $\sqcap_i \mathsf{T}_i^{\#}$ then it also belongs to some $\mathsf{T}_i^{\#}$.
- Let γ : **Independ** $\to \mathcal{P}(\mathbf{Trc})$ be defined as:

$$\gamma(\mathsf{T}^{\#}) = \{\mathsf{T} \in \mathbf{Trc} \mid \mathsf{T} \models \mathsf{T}^{\#}\}$$

- We can show that γ is completely multiplicative.
- Therefore, with $\alpha : \mathcal{P}(\mathbf{Trc}) \to$ **Independ** defined as: $\alpha(\mathsf{T}) = \bigcup\{\mathsf{T}^{\#} \mid \mathsf{T} \subseteq \gamma(\mathsf{T}^{\#})\}$, we have $(\mathcal{P}(\mathbf{Trc}), \alpha, \gamma,$ **Independ**$)$ is a Galois connection.