Information Flow Analysis
The semantics of a command has functionality \([\cdot] : C \rightarrow T_{rc}\).

For expressions, we assume there exists a semantic function

For expressions, we assume there exists a semantic function

Langauge, Semantics
Semantics, contd.

\[ x := E \]

\[ \text{let } s_0 = T s \text{ in } \]

\[ \text{if } E \text{ then } C \text{ else } C \]

\[ \text{while } E \text{ do } C \]

\[ \text{if } \text{true?} \text{ (} E \text{)} s_0 \text{ then } f(C) s \text{ else } s_0 \]

\[ \text{where } (f) = \text{lfp} \]

\( F: (\text{Trc} ! \text{Trc}) ! (\text{Trc} ! \text{Trc}) \)
We will be interested in finite abstractions of the pre-traces and the post-traces relevant to the execution of a command.

The abstract traces are termed independences: an independence 

\[ \text{independ} \subseteq \text{Var} \times ((\{\top\} \cap \text{Var})) \]

\[ \text{if } x \text{ is } \top \text{, then the nontermination behavior of the command is independent of } \text{initial value of } w. \]

\[ \text{if } x \text{ is a variable, then } [x \times [w]]_x \text{ denotes that the current value of } x \text{ is independent of the initial value of } w. \]

\[ \text{when an independence correctly describes a set of traces.} \]
Denote the greatest lower bound (which is the set union).

**Independence** forms a complete lattice wrt. the ordering \( \subseteq \). Let \( \#_T \).

The ordering \( \#_1 \preceq \#_2 \) holds iff for all \([x \times w] \in T#_1\) it holds that \( T#_1 \preceq T#_2 \).

For all \( T \in T_{RC} \), for all \( x \in \text{VAR} \), \( \{x\} \cap \{w\} = \{w\} \cup \{x\} \).

**Independence** of independences, ordering on.
Some facts

\[ T_j = T_{\#1} \quad \text{and} \quad T_{\#1} = T_{\#2} \quad \text{then} \quad T_j = T_{\#2}. \]

\[ \text{If for all } i \in I \text{ it holds that } T_j = T_{\#i} \text{, then } T_j = u_{i \in I} T_{\#i}. \]

\[ \text{If } T_j \models T_{\#1} \text{ and } T_{\#1} > T_{\#2} \text{ then } T_j \models T_{\#2}. \]
Is a Galois connection.

Let \( \lambda : \mathcal{P}(\mathcal{T}(\text{rc})) \to \text{Indep} \) be defined as:

\[
\{ \# \mathcal{T} \models \mathcal{T} \models \mathcal{T}(\text{rc}) \mid \mathcal{T} \models \_ \}\lambda = \lambda(\mathcal{T})
\]

Therefore, with \( \alpha : \mathcal{P}(\mathcal{T}(\text{rc})) \to \text{Indep} \) defined as:

We can show that \( \lambda \) is completely multiplicative.

If \( \mathcal{T} \) belongs to some \( \mathcal{T}(\text{rc}) \), then \( \mathcal{T} \) also belongs to some \( \mathcal{T}(\text{rc}) \).

Do we have an abstract interpretation?