Transitional Semantics

State transition sequence

$$s_0 \hookrightarrow s_1 \hookrightarrow s_2 \hookrightarrow \cdots$$

where $\hookrightarrow$ is a transition relation between states $\mathbb{S}$

$$\hookrightarrow \subseteq \mathbb{S} \times \mathbb{S}$$

A state $s \in \mathbb{S}$ of the program is a pair (l, m) of a program label l and the machine state m at that program label during execution.

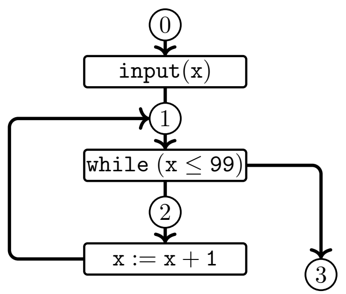
Concrete Transition Sequence

Example

Consider the following program

$$\begin{array}{l}\texttt{input}(\mathrm{x});\\ \texttt{while}\ (\mathrm{x} \leq 99)\\ \qquad \{\mathrm{x} := \mathrm{x} + 1\}\end{array}$$

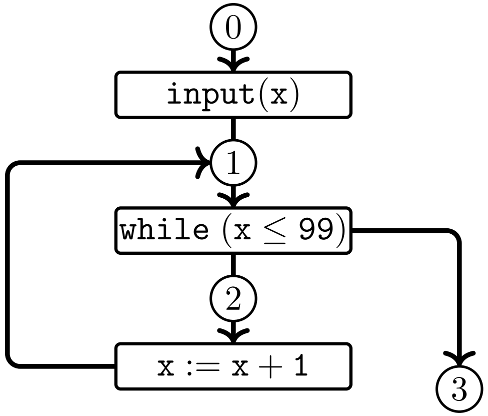
Let labels be "program points."



Let the initial state be $\emptyset$. Some transition sequences are:

For input 100: $(0, \emptyset) \hookrightarrow (1, x \mapsto 100) \hookrightarrow (3, x \mapsto 100)$.
For input 99: $(0, \emptyset) \hookrightarrow (1, x \mapsto 99) \hookrightarrow (2, x \mapsto 99) \hookrightarrow (1, x \mapsto 100) \hookrightarrow (3, x \mapsto 100)$.
For input 0: $(0, \emptyset) \hookrightarrow (1, x \mapsto 0) \hookrightarrow (2, x \mapsto 0) \hookrightarrow (1, x \mapsto 1) \hookrightarrow \cdots \hookrightarrow (3, x \mapsto 100)$.

Reachable States



Assume that the possible inputs are 0, 99, and 100. Then, the set of all reachable states are the set of states occurring in the three transition sequences:

$$
\begin{array}{ll}
 & \{(0,\emptyset),(1,x\mapsto 100),(3,x\mapsto 100)\} \\
\cup & \{(0,\emptyset),(1,x\mapsto 99),(2,x\mapsto 99),(1,x\mapsto 100),(3,x\mapsto 100)\} \\
\cup & \{(0,\emptyset),(1,x\mapsto 0),(2,x\mapsto 0),(1,x\mapsto 1),\cdots,(2,x\mapsto 99),(1,x\mapsto 100),(3,x\mapsto 100)\} \\
= & \{(0,\emptyset),(1,x\mapsto 0),\cdots,(1,x\mapsto 100),(2,x\mapsto 0),\cdots,(2,x\mapsto 99),(3,x\mapsto 100)\}
\end{array}
$$

Concrete Semantics: the Set of Reachable States (1/3)

Given a program, let I be the set of its initial states and *Step* be the powerset-lifted version of $\hookrightarrow$:

$$\begin{array}{l} \textit{Step} : \wp(\mathbb{S}) \to \wp(\mathbb{S}) \\ \textit{Step}(X) = \{s' \mid s \hookrightarrow s', s \in X\} \end{array}$$

The set of reachable states is

$$I \,\cup\, \textit{Step}^1(I) \,\cup\, \textit{Step}^2(I) \,\cup\, \cdots .$$

which is, equivalently, the limit of C_is

$$\begin{array}{rcl} C_0 & = & I \\ C_{i+1} & = & I \,\cup\, \textit{Step}(C_i) \end{array}$$

which is, the least solution of

$$X = I \,\cup\, \textit{Step}(X).$$

Concrete Semantics: the Set of Reachable States (2/3)

The least solution of

$$X = I \cup \mathit{Step}(X)$$

is also called *the least fixpoint* of F

$$\begin{array}{l} F : \wp(\mathbb{S}) \rightarrow \wp(\mathbb{S}) \\ F(X) = I \cup \mathit{Step}(X) \end{array}$$

written as

$$\mathbf{lfp} F.$$

Theorem (Least fixpoint)

The least fixpoint $\mathbf{lfp} F$ *of* $F(X) = I \cup \mathit{Step}(X)$ *is*

$$\bigcup_{i \geq 0} F^i(\emptyset)$$

where $F^0(X) = X$ *and* $F^{n+1}(X) = F(F^n(X))$.

Concrete Semantics: the Set of Reachable States (3/3)

Definition (Concrete semantics, the set of reachable states)

Given a program, let $\mathbb{S}$ be the set of states and $\hookrightarrow$ be the one-step transition relation $\subseteq \mathbb{S} \times \mathbb{S}$. Let I be the set of its initial states and *Step* be the powerset-lifted version of $\hookrightarrow$:

$$\begin{array}{l} \mathit{Step} : \wp(\mathbb{S}) \to \wp(\mathbb{S}) \\ \mathit{Step}(X) = \{s' \mid s \hookrightarrow s', s \in X\}. \end{array}$$

Then the concrete semantics of the program, the set of all reachable states from I, is defined as the least fixpoint $\mathbf{lfp}F$ of F

$$F(X) = I \cup \mathit{Step}(X).$$

Analysis Goal

Program-label-wise reachability

For each program label we want to know the set of memories that can occur at that label during executions of the input program.

- labels: "partitioning indices"
- e.g., statement labels as in programs, statement labels after loop unrolling, statement labels after function inlining