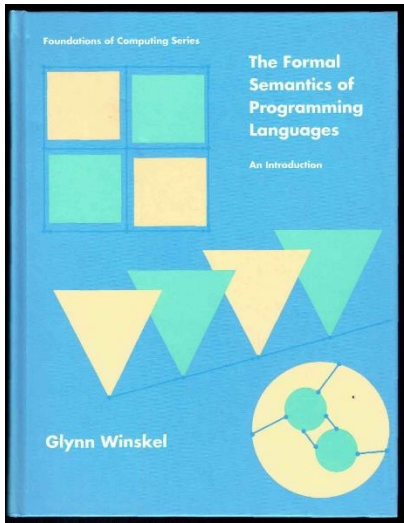
Advanced Topics in Programming Languages

Denotational and Axiomatic Semantics

Reference:

Winskel: The Formal Semantics of Programming Languages

Chapter 5,6



Axiomatic Semantics

Hoare Proof Rules for Partial Correctness

$$\{A\}\ \text{skip}\ \{A\}$$

$$\{B[a/X]\}\ X:=a\ \{B\}$$

$$\frac{\{P\}\ c_0\ \{C\}\ \{C\}\ c_1\ \{Q\}}{\{P\}\ c_0;c_1\{Q\}}$$

$$\frac{\{P \wedge b\}\ c_0\ \{Q\}\ \{P \wedge \neg b\}\ c_1\ \{Q\}}{\{P\}\ \text{if b then } c_0 \text{ else } c_1\{Q\}}$$

$$\frac{\{I \wedge b\}\ c\ \{I\}}{\{I\}\ \text{while b do c}\{I \wedge \neg b\}}$$

$$\frac{\models P \Rightarrow P' \qquad \{P'\}\ c\ \{Q'\} \qquad \models Q' \Rightarrow Q}{\{P\}\ c\ \{Q\}}$$

Standard Exponentiation

$\{n \geq 0\}$

r := 1;

e := n;

while e > 0 do (

    r := r * x;

    e := e – 1;

)

$\{r = x^n\}$

Standard Exponentiation

$\{0 \leq n\}$

r := 1;

$\{0 \leq n \wedge r=1\}$

e := n;

$\{0 \leq n \wedge r=1 \wedge e=n\}$

while e > 0 do $\{0 \leq n \wedge 0 \leq e \wedge r = x^{n-e}\}$ (

  r := r * x;

  $\{0 \leq n \wedge 0 < e \wedge r = x^{n-e+1}\}$

  e := e – 1;

)

$\{r = x^n\}$

Fast Exponentiation

$\{n \geq 0\}$

```
r := 1;
p := x;
e := n;
while e > 0 do (
    if (e mod 2 = 1) then (r := r * p) else (skip);
    p := p * p;
    e := e div 2;
)
```

$\{r = x^n\}$

Connection between Natural Operational Semantics and Denotational Semantics

Abstract Syntax for IMP

Aexp $a ::= n \mid X \mid a_0 + a_1 \mid a_0 - a_1 \mid a_0 \times a_1$

Bexp $b ::= \text{true} \mid \text{false} \mid a_0 = a_1 \mid a_0 \leq a_1 \mid \neg b \mid b_0 \wedge b_1 \mid b_0 \vee b_1$

Com $c ::= \text{skip} \mid X := a \mid c_0 ; c_1 \mid \text{if } b \text{ then } c_0 \text{ else } c_1 \mid \text{while } b \text{ do } c$

Natural Operational Semantics: Aexp

- $\langle n, \sigma \rangle \rightarrow n$
- $\langle X, \sigma \rangle \rightarrow \sigma(X)$
- $$\frac{< a_0, \sigma > \rightarrow n_0, < a_1, \sigma > \rightarrow n_1}{< a_0 + a_1, \sigma > \rightarrow n} \; where \quad n = n_0 + n_1$$
- $$\frac{< a_0, \sigma > \rightarrow n_0, < a_1, \sigma > \rightarrow n_1}{< a_0 - a_1, \sigma > \rightarrow n} \; where \quad n = n_0 - n_1$$
- $$\frac{< a_0, \sigma > \rightarrow n_0, < a_1, \sigma > \rightarrow n_1}{< a_0 \times a_1, \sigma > \rightarrow n} \; where \quad n = n_0 \times n_1$$

Natural Operational Semantics: Bexp

- **<true, σ>** $\rightarrow$ **true**
- **<false, σ>** $\rightarrow$ **false**
- $$\frac{< a_0, \sigma > \rightarrow n, < a_1, \sigma > \rightarrow m}{< a_0 = a_1, \sigma > \rightarrow \mathbf{true}} \; if \quad n = m$$
- $$\frac{< a_0, \sigma > \rightarrow n, < a_1, \sigma > \rightarrow m}{< a_0 = a_1, \sigma > \rightarrow \mathbf{false}} \; if \quad n \neq m$$
- $$\frac{< a_0, \sigma > \rightarrow n, < a_1, \sigma > \rightarrow m}{< a_0 \leq a_1, \sigma > \rightarrow \mathbf{true}} \; if \quad n \leq m$$
- $$\frac{< a_0, \sigma > \rightarrow n, < a_1, \sigma > \rightarrow m}{< a_0 \leq a_1, \sigma > \rightarrow \mathbf{false}} \; if \; not \quad n \leq m$$

Natural Operational Semantics: Bexp

- $$\frac{< b, \sigma > \rightarrow \textbf{true}}{< \neg b, \sigma > \rightarrow \textbf{false}}$$
- $$\frac{< b, \sigma > \rightarrow \textbf{false}}{< \neg b, \sigma > \rightarrow \textbf{true}}$$
- $$\frac{< b_0, \sigma > \rightarrow t_0, < b_1, \sigma > \rightarrow t_1}{< b_0 \wedge b_1, \sigma > \rightarrow t}$$ where $t = \textbf{true}$ when $t_0 = t_1 = \textbf{true}$ and $t = \textbf{false}$ otherwise
- $$\frac{< b_0, \sigma > \rightarrow t_0, < b_1, \sigma > \rightarrow t_1}{< b_0 \vee b_1, \sigma > \rightarrow t}$$ where $t = \textbf{false}$ when $t_0 = t_1 = \textbf{false}$ and $t = \textbf{true}$ otherwise

Natural Operational Semantics: Com

$$\langle \textbf{skip}, \sigma \rangle \rightarrow \sigma$$

$$\frac{\langle a, \sigma \rangle \rightarrow n}{\langle X := a, \sigma \rangle \rightarrow \sigma[n/X]}$$

$$\frac{\langle c0, \sigma \rangle \rightarrow \sigma'' \quad \langle c1, \sigma'' \rangle \rightarrow \sigma'}{\langle c_0 \,;\, c_1, \sigma \rangle \rightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \rightarrow \textbf{true} \quad \langle c_0, \sigma \rangle \rightarrow \sigma'}{\langle \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1, \sigma \rangle \rightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \rightarrow \textbf{false} \quad \langle c_1, \sigma \rangle \rightarrow \sigma'}{\langle \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1, \sigma \rangle \rightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \rightarrow \textbf{false}}{\langle \textbf{while } b \textbf{ do } c, \sigma \rangle \rightarrow \sigma}$$

$$\frac{\langle b, \sigma \rangle \rightarrow \textbf{true} \quad \langle \textbf{c}, \sigma \rangle \rightarrow \sigma'' \quad \langle \textbf{while } b \textbf{ do } c, \sigma'' \rangle \rightarrow \sigma'}{\langle \textbf{while } b \textbf{ do } c, \sigma \rangle \rightarrow \sigma'}$$

Natural Operational Semantics: Summary

- $\rightarrow_A \subseteq \text{Aexp} \times \Sigma \times \mathbb{N}$ $\quad\quad$ $\langle a, \sigma \rangle \rightarrow n$
- $\rightarrow_B \subseteq \text{Bexp} \times \Sigma \times T$ $\quad\quad$ $\langle b, \sigma \rangle \rightarrow t$
- $\rightarrow_C \subseteq \text{Com} \times \Sigma \times \Sigma$ $\quad\quad$ $\langle c, \sigma \rangle \rightarrow \sigma'$

Denotational Semantics: Aexp

- **A:** $\text{Aexp} \to (\Sigma \to \text{N})$
- $\mathbf{A}[\![n]\!] = \{(\sigma, n) \mid \sigma \in \Sigma\}$
- $\mathbf{A}[\![X]\!] = \{(\sigma, \sigma(X)) \mid \sigma \in \Sigma\}$
- $\mathbf{A}[\![a_0+a_1]\!] = \{(\sigma, n_0+n_1) \mid (\sigma, n_0) \in \mathbf{A}[\![a_0]\!], (\sigma, n_1) \in \mathbf{A}[\![a_1]\!]\}$
- $\mathbf{A}[\![a_0-a_1]\!] = \{(\sigma, n_0-n_1) \mid (\sigma, n_0) \in \mathbf{A}[\![a_0]\!], (\sigma, n_1) \in \mathbf{A}[\![a_1]\!]\}$
- $\mathbf{A}[\![a_0 \times a_1]\!] = \{(\sigma, n_0 \times n_1) \mid (\sigma, n_0) \in \mathbf{A}[\![a_0]\!], (\sigma, n_1) \in \mathbf{A}[\![a_1]\!]\}$

Denotational Semantics: Bexp

- **B:** Bexp $\rightarrow (\Sigma \rightarrow T)$
- **B** $[\![\text{true}]\!] = \{(\sigma, \text{true}) \mid \sigma \in \Sigma\}$
- **B** $[\![\text{false}]\!] = \{(\sigma, \text{false}) \mid \sigma \in \Sigma\}$
- **B** $[\![a_0 = a_1]\!] = \{(\sigma, \text{true}) \mid \sigma \in \Sigma \;\&\; \mathbf{A}[\![a_0]\!]\sigma = \mathbf{A}[\![a_1]\!]\sigma\} \cup$
  $\{(\sigma, \text{false}) \mid \sigma \in \Sigma \;\&\; \mathbf{A}[\![a_0]\!]\sigma \neq \mathbf{A}[\![a_1]\!]\sigma\}$
- **B** $[\![a_0 \leq a_1]\!] = \{(\sigma, \text{true}) \mid \sigma \in \Sigma \;\&\; \mathbf{A}[\![a_0]\!]\sigma \leq \mathbf{A}[\![a_1]\!]\sigma\} \cup$
  $\{(\sigma, \text{false}) \mid \sigma \in \Sigma \;\&\; \mathbf{A}[\![a_0]\!]\sigma \not\leq \mathbf{A}[\![a_1]\!]\sigma\}$
- **B** $[\![\neg b]\!] = \{(\sigma, \neg_T t) \mid \sigma \in \Sigma, (\sigma, t) \in \mathbf{B}[\![b]\!]\}$
- **B** $[\![b_0 \wedge b_1]\!] = \{(\sigma, t_0 \wedge_T t_1) \mid \sigma \in \Sigma, (\sigma, t_0) \in \mathbf{B}[\![b_0]\!], (\sigma, t_1) \in \mathbf{B}[\![b_1]\!]\}$
- **B** $[\![b_0 \vee b_1]\!] = \{(\sigma, t_0 \vee_T t_1) \mid \sigma \in \Sigma, (\sigma, t_0) \in \mathbf{B}[\![b_0]\!], (\sigma, t_1) \in \mathbf{B}[\![b_1]\!]\}$

Denotational Semantics: Com

- $X_\perp = X \cup \{\perp\}$
- **C:** Com $\rightarrow (\Sigma_\perp \rightarrow \Sigma_\perp)$
- $\mathbf{C}[\![\text{skip}]\!] = \{(\perp, \perp)\} \cup \{(\sigma, \sigma) \mid \sigma \in \Sigma\}$
- $\mathbf{C}[\![X:=a]\!] = \{(\perp, \perp)\} \cup \{(\sigma, \sigma[n/X]) \mid \sigma \in \Sigma \;\&\; n = \mathbf{A}[\![a]\!]\sigma\}$
- $\mathbf{C}[\![c_0;c_1]\!] = \mathbf{C}[\![c_0]\!] \circ \mathbf{C}[\![c_1]\!] = \{(\sigma, \sigma'') \mid (\sigma, \sigma') \in \mathbf{C}[\![c_0]\!] \;\&\; (\sigma', \sigma'') \in \mathbf{C}[\![c_1]\!]\}$
- $\mathbf{C}[\![\text{if b then } c_0 \text{ else } c_1]\!] =$ $\{(\perp, \perp)\} \cup$
  $\{(\sigma, \sigma') \mid (\sigma, \sigma') \in \mathbf{C}[\![c_0]\!] \;\&\; \mathbf{B}[\![a]\!]\sigma = \text{true}\} \cup$
  $\{(\sigma, \sigma') \mid (\sigma, \sigma') \in \mathbf{C}[\![c_1]\!] \;\&\; \mathbf{B}[\![a]\!]\sigma = \text{false}\}$
- $\mathbf{C}[\![\text{while b do c}]\!] = \text{lfp}(F) = \bigsqcup F^k(\perp)$ where $F:[[\sum_\perp \rightarrow \sum_\perp] \rightarrow [\sum_\perp \rightarrow \sum_\perp]]$

$$F(w) = \lambda\sigma. \begin{cases} w\,(C[\![c]\!]\sigma) & \text{if } B[\![b]\!]\sigma = \text{true} \\ \sigma & \text{if } B[\![b]\!]\sigma = \text{false} \\ \perp & \text{if } \sigma = \perp \end{cases}$$

Posets, CPO's, PCPO's

- A partial order is reflexive, transitive, and antisymmetric
  - $\forall x.\, x \sqsubseteq x$
  - $\forall x, y, z.\ x \sqsubseteq y \wedge y \sqsubseteq z \rightarrow x \sqsubseteq z$
  - $\forall x, y.\, x \sqsubseteq y \wedge y \sqsubseteq x \rightarrow x = y$
- A chain is a countable increasing sequence: $x_0 \sqsubseteq x_1 \sqsubseteq \ldots$
- CPO (complete partial order): every chain has a least upper bound
  - $x_j \sqsubseteq \bigsqcup \langle x_i \rangle$ for all $j \in N$
  - $\bigsqcup \langle x_i \rangle \sqsubseteq y$ for all upper bounds y of $\langle x_i \rangle$
  - $\bigsqcup \langle x_i \rangle$ is unique if it exists
- PCPO (pointed CPO) is a CPO with a least element $\perp$
- If S is a set, and E is a PCPO, then so is $S \rightarrow E$
  - $m \sqsubseteq m'$ iff $\forall s \in S$: $m(s) \sqsubseteq_E m'(s)$
  - $\perp_{S \rightarrow E} = \lambda s.\, \perp_E$
  - $\bigsqcup (m , m') = \lambda s.m(s) \bigsqcup_E m'(s)$

Natural Operational Semantics ⇔ Denotational Semantics

- Natural Operational Semantics:

  $\rightarrow_A \subseteq \mathrm{Aexp} \times \Sigma \times \mathbb{N}$ $\quad$ $\langle a, \sigma \rangle \rightarrow n$

  $\rightarrow_B \subseteq \mathrm{Bexp} \times \Sigma \times T$ $\quad$ $\langle b, \sigma \rangle \rightarrow t$

  $\rightarrow_C \subseteq \mathrm{Com} \times \Sigma \times \Sigma$ $\quad$ $\langle c, \sigma \rangle \rightarrow \sigma'$

- Denotational Semantics:

  A: Aexp $\rightarrow (\Sigma \rightarrow \mathbb{N})$

  B: Bexp $\rightarrow (\Sigma \rightarrow T)$

  C: Com $\rightarrow (\Sigma_\perp \rightarrow \Sigma_\perp)$

- What is the connection? How to formalize?
- Proof: whiteboard (section 5.3 of Winskel)