Semantics and Verification of Software

Lecture 6: Denotational Semantics of WHILE II (Chain-Complete Partial Orders)

Thomas Noll

Lehrstuhl für Informatik 2
(Software Modeling and Verification)

RWTH AACHEN UNIVERSITY

noll@cs.rwth-aachen.de

http://www-i2.informatik.rwth-aachen.de/i2/svsw11/

Winter Semester 2011/12

Outline

Definition (Denotational semantics of statements)

The (denotational) semantic functional for statements,

$$\mathfrak{C}[\![.]\!] : Cmd \to (\Sigma \dashrightarrow \Sigma),$$

is given by:

$$\begin{aligned}
\mathfrak{C}[\![\texttt{skip}]\!] &:= \mathrm{id}_\Sigma \\
\mathfrak{C}[\![x \texttt{ := } a]\!]\sigma &:= \sigma[x \mapsto \mathfrak{A}[\![a]\!]\sigma] \\
\mathfrak{C}[\![c_1 \,;\, c_2]\!] &:= \mathfrak{C}[\![c_2]\!] \circ \mathfrak{C}[\![c_1]\!] \\
\mathfrak{C}[\![\texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2]\!] &:= \mathrm{cond}(\mathfrak{B}[\![b]\!], \mathfrak{C}[\![c_1]\!], \mathfrak{C}[\![c_2]\!]) \\
\mathfrak{C}[\![\texttt{while } b \texttt{ do } c]\!] &:= \mathrm{fix}(\Phi)
\end{aligned}$$

where $\Phi : (\Sigma \dashrightarrow \Sigma) \to (\Sigma \dashrightarrow \Sigma) : f \mapsto \mathrm{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \mathrm{id}_\Sigma)$

Why Fixpoints?

- Goal: preserve validity of equivalence
  $$\mathfrak{C}[\![\texttt{while}\ b\ \texttt{do}\ c]\!] \overset{(*)}{=} \mathfrak{C}[\![\texttt{if}\ b\ \texttt{then}\ (c\texttt{;while}\ b\ \texttt{do}\ c)\ \texttt{else skip}]\!]$$
  (cf. Lemma 4.3)
- Using the known parts of Def. 5.3, we obtain:
  $$\begin{aligned}
  &\mathfrak{C}[\![\texttt{while}\ b\ \texttt{do}\ c]\!]\\
  \overset{(*)}{=}\ &\mathfrak{C}[\![\texttt{if}\ b\ \texttt{then}\ (c\texttt{;while}\ b\ \texttt{do}\ c)\ \texttt{else skip}]\!]\\
  \overset{\text{Def. 5.3}}{=}\ &\mathrm{cond}(\mathfrak{B}[\![b]\!], \mathfrak{C}[\![c\texttt{;while}\ b\ \texttt{do}\ c]\!], \mathfrak{C}[\![\texttt{skip}]\!])\\
  \overset{\text{Def. 5.3}}{=}\ &\mathrm{cond}(\mathfrak{B}[\![b]\!], \mathfrak{C}[\![\texttt{while}\ b\ \texttt{do}\ c]\!] \circ \mathfrak{C}[\![c]\!], \mathrm{id}_\Sigma)
  \end{aligned}$$
- Abbreviating $f := \mathfrak{C}[\![\texttt{while}\ b\ \texttt{do}\ c]\!]$ this yields:
  $$f = \mathrm{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \mathrm{id}_\Sigma)$$
- Hence f must be a solution of this recursive equation
- In other words: f must be a fixpoint of the mapping
  $$\Phi : (\Sigma \dashrightarrow \Sigma) \to (\Sigma \dashrightarrow \Sigma) : f \mapsto \mathrm{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \mathrm{id}_\Sigma)$$
  (since the equation can be stated as $f = \Phi(f)$)

Characterization of $\text{fix}(\Phi)$

For $\Phi(f_0) = f_0$ and initial state $\sigma_0 \in \Sigma$, case distinction yields:

1. Loop `while` b `do` c terminates after n iterations ($n \in \mathbb{N}$)
   $\implies f_0(\sigma_0) = \sigma_n$
2. Body c diverges in the nth iteration
   $\implies f_0(\sigma_0) = \text{undefined}$
3. Loop `while` b `do` c diverges
   $\implies$ no condition on f_0 (only $f_0(\sigma_0) = f_0(\sigma_i)$ for every $i \in \mathbb{N}$)

- Not surprising since, e.g., for the loop `while true do skip` every $f : \Sigma \dashrightarrow \Sigma$ is a fixpoint:

$$\Phi(f) = \text{cond}(\mathfrak{B}[\![\text{true}]\!], f \circ \mathfrak{C}[\![\texttt{skip}]\!], \text{id}_\Sigma) = f$$

- On the other hand, our operational understanding requires, for every $\sigma_0 \in \Sigma$,

$$\mathfrak{C}[\![\texttt{while true do skip}]\!]\sigma_0 = \text{undefined}$$

Conclusion

$\text{fix}(\Phi)$ is the least defined fixpoint of Φ.

Outline

Making It Precise I

To use fixpoint theory, the notion of "least defined" has to be made precise.

- Given $f, g : \Sigma \dashrightarrow \Sigma$, let

$$f \sqsubseteq g \iff \text{for every } \sigma, \sigma' \in \Sigma : f(\sigma) = \sigma' \implies g(\sigma) = \sigma'$$

  (g is "at least as defined" as f)

To use fixpoint theory, the notion of "least defined" has to be made precise.

- Given $f, g : \Sigma \dashrightarrow \Sigma$, let

$$f \sqsubseteq g \iff \text{for every } \sigma, \sigma' \in \Sigma : f(\sigma) = \sigma' \implies g(\sigma) = \sigma'$$

  (g is "at least as defined" as f)
- Equivalent to requiring

$$\text{graph}(f) \subseteq \text{graph}(g)$$

  where

$$\text{graph}(h) := \{(\sigma, \sigma') \mid \sigma \in \Sigma, \sigma' = h(\sigma) \text{ defined}\} \subseteq \Sigma \times \Sigma$$

  for every $h : \Sigma \dashrightarrow \Sigma$

Making It Precise II

Example 6.1

Let $x \in Var$ be fixed, and let $f_0, f_1, f_2, f_3 : \Sigma \dashrightarrow \Sigma$ be given by

$$
\begin{aligned}
f_0(\sigma) &:= \text{undefined} \\
f_1(\sigma) &:= \begin{cases} \sigma & \text{if } \sigma(x) \text{ even} \\ \text{undefined} & \text{otherwise} \end{cases} \\
f_2(\sigma) &:= \begin{cases} \sigma & \text{if } \sigma(x) \text{ odd} \\ \text{undefined} & \text{otherwise} \end{cases} \\
f_3(\sigma) &:= \sigma
\end{aligned}
$$

Making It Precise II

Example 6.1

Let $x \in Var$ be fixed, and let $f_0, f_1, f_2, f_3 : \Sigma \dashrightarrow \Sigma$ be given by

$$
\begin{aligned}
f_0(\sigma) &:= \text{undefined} \\
f_1(\sigma) &:= \begin{cases} \sigma & \text{if } \sigma(x) \text{ even} \\ \text{undefined} & \text{otherwise} \end{cases} \\
f_2(\sigma) &:= \begin{cases} \sigma & \text{if } \sigma(x) \text{ odd} \\ \text{undefined} & \text{otherwise} \end{cases} \\
f_3(\sigma) &:= \sigma
\end{aligned}
$$

This implies $f_0 \sqsubseteq f_1 \sqsubseteq f_3$, $f_0 \sqsubseteq f_2 \sqsubseteq f_3$, $f_1 \not\sqsubseteq f_2$, and $f_2 \not\sqsubseteq f_1$

Characterization of $\text{fix}(\Phi)$ I

Now $\text{fix}(\Phi)$ can be characterized by:

- $\text{fix}(\Phi)$ is a fixpoint of Φ, i.e.,

$$\Phi(\text{fix}(\Phi)) = \text{fix}(\Phi)$$

- $\text{fix}(\Phi)$ is minimal with respect to $\sqsubseteq$, i.e., for every $f_0 : \Sigma \dashrightarrow \Sigma$ such that $\Phi(f_0) = f_0$,

$$\text{fix}(\Phi) \sqsubseteq f_0$$

Characterization of fix(Φ) I

Now fix(Φ) can be characterized by:

- fix(Φ) is a fixpoint of Φ, i.e.,

$$\Phi(\mathrm{fix}(\Phi)) = \mathrm{fix}(\Phi)$$

- fix(Φ) is minimal with respect to $\sqsubseteq$, i.e., for every $f_0 : \Sigma \dashrightarrow \Sigma$ such that $\Phi(f_0) = f_0$,

$$\mathrm{fix}(\Phi) \sqsubseteq f_0$$

Example 6.2

For `while true do skip` we obtain for every $f : \Sigma \dashrightarrow \Sigma$:

$$\Phi(f) = \mathrm{cond}(\mathfrak{B}[\![\mathtt{true}]\!], f \circ \mathfrak{C}[\![\mathtt{skip}]\!], \mathrm{id}_\Sigma) = f$$

Characterization of fix(Φ) I

Now fix(Φ) can be characterized by:

- fix(Φ) is a fixpoint of Φ, i.e.,

$$\Phi(\mathrm{fix}(\Phi)) = \mathrm{fix}(\Phi)$$

- fix(Φ) is minimal with respect to $\sqsubseteq$, i.e., for every $f_0 : \Sigma \dashrightarrow \Sigma$ such that $\Phi(f_0) = f_0$,

$$\mathrm{fix}(\Phi) \sqsubseteq f_0$$

Example 6.2

For `while true do skip` we obtain for every $f : \Sigma \dashrightarrow \Sigma$:

$$\Phi(f) = \mathrm{cond}(\mathfrak{B}[\![\mathrm{true}]\!], f \circ \mathfrak{C}[\![\mathtt{skip}]\!], \mathrm{id}_\Sigma) = f$$

$\Longrightarrow$ $\mathrm{fix}(\Phi) = f_\emptyset$ where $f_\emptyset(\sigma) :=$ undefined for every $\sigma \in \Sigma$
(that is, $\mathrm{graph}(f_\emptyset) = \emptyset$)

Characterization of $\mathrm{fix}(\Phi)$ II

Goals:

- Prove existence of $\mathrm{fix}(\Phi)$ for $\Phi(f) = \mathrm{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \mathrm{id}_\Sigma)$
- Show how it can be "computed" (more exactly: approximated)

Characterization of $\mathrm{fix}(\Phi)$ II

Goals:

- Prove existence of $\mathrm{fix}(\Phi)$ for $\Phi(f) = \mathrm{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \mathrm{id}_\Sigma)$
- Show how it can be "computed" (more exactly: approximated)

Sufficient conditions:

on domain $\Sigma \dashrightarrow \Sigma$: chain-complete partial order

on function Φ: continuity

Outline

Partial Orders

Definition 6.1 (Partial order)

A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \; \subseteq \; D \times D$ such that, for every $d_1, d_2, d_3 \in D$,

reflexivity: $d_1 \sqsubseteq d_1$

transitivity: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \implies d_1 \sqsubseteq d_3$

antisymmetry: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \implies d_1 = d_2$

It is called total if, in addition, always $d_1 \sqsubseteq d_2$ or $d_2 \sqsubseteq d_1$.

Partial Orders

Definition 6.1 (Partial order)

A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \subseteq D \times D$ such that, for every $d_1, d_2, d_3 \in D$,

reflexivity: $d_1 \sqsubseteq d_1$

transitivity: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \implies d_1 \sqsubseteq d_3$

antisymmetry: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \implies d_1 = d_2$

It is called total if, in addition, always $d_1 \sqsubseteq d_2$ or $d_2 \sqsubseteq d_1$.

Example 6.2

1. $(\mathbb{N}, \leq)$ is a total partial order

Partial Orders

Definition 6.1 (Partial order)

A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \subseteq D \times D$ such that, for every $d_1, d_2, d_3 \in D$,

reflexivity: $d_1 \sqsubseteq d_1$

transitivity: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \implies d_1 \sqsubseteq d_3$

antisymmetry: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \implies d_1 = d_2$

It is called total if, in addition, always $d_1 \sqsubseteq d_2$ or $d_2 \sqsubseteq d_1$.

Example 6.2

1. $(\mathbb{N}, \leq)$ is a total partial order
2. $(2^{\mathbb{N}}, \subseteq)$ is a (non-total) partial order

Partial Orders

Definition 6.1 (Partial order)

A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \subseteq D \times D$ such that, for every $d_1, d_2, d_3 \in D$,

reflexivity: $d_1 \sqsubseteq d_1$

transitivity: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \implies d_1 \sqsubseteq d_3$

antisymmetry: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \implies d_1 = d_2$

It is called total if, in addition, always $d_1 \sqsubseteq d_2$ or $d_2 \sqsubseteq d_1$.

Example 6.2

1. $(\mathbb{N}, \leq)$ is a total partial order
2. $(2^{\mathbb{N}}, \subseteq)$ is a (non-total) partial order
3. $(\mathbb{N}, <)$ is not a partial order

Partial Orders

Definition 6.1 (Partial order)

A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \subseteq D \times D$ such that, for every $d_1, d_2, d_3 \in D$,

reflexivity: $d_1 \sqsubseteq d_1$

transitivity: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \implies d_1 \sqsubseteq d_3$

antisymmetry: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \implies d_1 = d_2$

It is called total if, in addition, always $d_1 \sqsubseteq d_2$ or $d_2 \sqsubseteq d_1$.

Example 6.2

1. $(\mathbb{N}, \leq)$ is a total partial order
2. $(2^{\mathbb{N}}, \subseteq)$ is a (non-total) partial order
3. $(\mathbb{N}, <)$ is not a partial order (since not reflexive)

Application to $\mathrm{fix}(\Phi)$ I

Lemma 6.3

$(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$ *is a partial order.*

Application to $\mathrm{fix}(\Phi)$ I

Lemma 6.3

$(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$ *is a partial order.*

Proof.

on the board □

Chains and Least Upper Bounds I

Definition 6.4 (Chain, (least) upper bound)

Let $(D, \sqsubseteq)$ be a partial order and $S \subseteq D$.

1. S is called a chain in D if, for every $s_1, s_2 \in S$,

$$s_1 \sqsubseteq s_2 \text{ or } s_2 \sqsubseteq s_1$$

(that is, S is a totally ordered subset of D).

Chains and Least Upper Bounds I

Definition 6.4 (Chain, (least) upper bound)

Let $(D, \sqsubseteq)$ be a partial order and $S \subseteq D$.

1. S is called a chain in D if, for every $s_1, s_2 \in S$,
$$s_1 \sqsubseteq s_2 \text{ or } s_2 \sqsubseteq s_1$$
(that is, S is a totally ordered subset of D).
2. An element $d \in D$ is called an upper bound of S if $s \sqsubseteq d$ for every $s \in S$ (notation: $S \sqsubseteq d$).

Definition 6.4 (Chain, (least) upper bound)

Let $(D, \sqsubseteq)$ be a partial order and $S \subseteq D$.

1. S is called a chain in D if, for every $s_1, s_2 \in S$,
$$s_1 \sqsubseteq s_2 \text{ or } s_2 \sqsubseteq s_1$$
(that is, S is a totally ordered subset of D).
2. An element $d \in D$ is called an upper bound of S if $s \sqsubseteq d$ for every $s \in S$ (notation: $S \sqsubseteq d$).
3. An upper bound d of S is called least upper bound (LUB) or supremum of S if $d \sqsubseteq d'$ for every upper bound d' of S (notation: $d = \bigsqcup S$).

Example 6.5

1. Every subset $S \subseteq \mathbb{N}$ is a chain in $(\mathbb{N}, \leq)$.
   It has a LUB (its greatest element) iff it is finite.

Chains and Least Upper Bounds II

Example 6.5

1. Every subset $S \subseteq \mathbb{N}$ is a chain in $(\mathbb{N}, \leq)$.
   It has a LUB (its greatest element) iff it is finite.
2. $\{\emptyset, \{0\}, \{0, 1\}, \ldots\}$ is a chain in $(2^{\mathbb{N}}, \subseteq)$ with LUB $\mathbb{N}$.

Chains and Least Upper Bounds II

Example 6.5

1. Every subset $S \subseteq \mathbb{N}$ is a chain in $(\mathbb{N}, \leq)$.
   It has a LUB (its greatest element) iff it is finite.
2. $\{\emptyset, \{0\}, \{0,1\}, \ldots\}$ is a chain in $(2^{\mathbb{N}}, \subseteq)$ with LUB $\mathbb{N}$.
3. Let $x \in Var$, and let $f_i : \Sigma \dashrightarrow \Sigma$ for every $i \in \mathbb{N}$ be given by

$$f_i(\sigma) := \begin{cases} \sigma[x \mapsto \sigma(x)+1] & \text{if } \sigma(x) \leq i \\ \text{undefined} & \text{otherwise} \end{cases}$$

   Then $\{f_0, f_1, f_2, \ldots\}$ is a chain in $(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$, since for every $i \in \mathbb{N}$ and $\sigma, \sigma' \in \Sigma$:

$$\begin{array}{ll} & f_i(\sigma) = \sigma' \\ \Longrightarrow & \sigma(x) \leq i, \sigma' = \sigma[x \mapsto \sigma(x)+1] \\ \Longrightarrow & \sigma(x) \leq i+1, \sigma' = \sigma[x \mapsto \sigma(x)+1] \\ \Longrightarrow & f_{i+1}(\sigma) = \sigma' \\ \Longrightarrow & f_i \sqsubseteq f_{i+1} \end{array}$$

Chain Completeness

Definition 6.6 (Chain completeness)

A partial order is called chain complete (CCPO) if every of its chains has a least upper bound.

Chain Completeness

Definition 6.6 (Chain completeness)

A partial order is called chain complete (CCPO) if every of its chains has a least upper bound.

Example 6.7

1. $(2^{\mathbb{N}}, \subseteq)$ is a CCPO with $\bigsqcup S = \bigcup_{M \in S} M$ for every chain $S \subseteq 2^{\mathbb{N}}$.

Chain Completeness

Definition 6.6 (Chain completeness)

A partial order is called chain complete (CCPO) if every of its chains has a least upper bound.

Example 6.7

1. $(2^{\mathbb{N}}, \subseteq)$ is a CCPO with $\bigsqcup S = \bigcup_{M \in S} M$ for every chain $S \subseteq 2^{\mathbb{N}}$.
2. $(\mathbb{N}, \leq)$ is not chain complete

Chain Completeness

Definition 6.6 (Chain completeness)

A partial order is called chain complete (CCPO) if every of its chains has a least upper bound.

Example 6.7

1. $(2^{\mathbb{N}}, \subseteq)$ is a CCPO with $\bigsqcup S = \bigcup_{M \in S} M$ for every chain $S \subseteq 2^{\mathbb{N}}$.
2. $(\mathbb{N}, \leq)$ is not chain complete
(since, e.g., the chain $\mathbb{N}$ has no upper bound).

Least Elements in CCPOs

Corollary 6.8

Every CCPO has a least element $\bigsqcup \emptyset$.

Corollary 6.8

Every CCPO has a least element $\bigsqcup \emptyset$.

Proof.

Let $(D, \sqsubseteq)$ be a CCPO.

- By definition, $\emptyset$ is a chain in D.

Least Elements in CCPOs

Corollary 6.8

Every CCPO has a least element $\bigsqcup \emptyset$.

Proof.

Let $(D, \sqsubseteq)$ be a CCPO.

- By definition, $\emptyset$ is a chain in D.
- By definition, every $d \in D$ is an upper bound of $\emptyset$.

Least Elements in CCPOs

Corollary 6.8

Every CCPO has a least element $\bigsqcup \emptyset$.

Proof.

Let $(D, \sqsubseteq)$ be a CCPO.

- By definition, $\emptyset$ is a chain in D.
- By definition, every $d \in D$ is an upper bound of $\emptyset$.
- Thus $\bigsqcup \emptyset$ exists and is the least element of D.

□

Application to $\text{fix}(\Phi)$ II

Lemma 6.9

- $(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$ *is a CCPO with least element* $f_\emptyset$ *where* $\text{graph}(f_\emptyset) = \emptyset$.
- *In particular, for every chain* $S \subseteq \Sigma \dashrightarrow \Sigma$,

$$\text{graph}\left(\bigsqcup S\right) = \bigcup_{f \in S} \text{graph}(f).$$

Lemma 6.9

- $(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$ *is a CCPO with least element* $f_\emptyset$ *where* $\mathrm{graph}(f_\emptyset) = \emptyset$.
- *In particular, for every chain* $S \subseteq \Sigma \dashrightarrow \Sigma$,

$$\mathrm{graph}\left(\bigsqcup S\right) = \bigcup_{f \in S} \mathrm{graph}(f).$$

Proof.

on the board □

Application to $\mathsf{fix}(\Phi)$ II

Lemma 6.9

- $(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$ *is a CCPO with least element* $f_\emptyset$ *where* $\mathsf{graph}(f_\emptyset) = \emptyset$.
- *In particular, for every chain* $S \subseteq \Sigma \dashrightarrow \Sigma$,
$$\mathsf{graph}\left(\bigsqcup S\right) = \bigcup_{f \in S} \mathsf{graph}(f).$$

Proof.

on the board □

Example 6.10 (cf. Example 6.5(3))

Let $x \in Var$, and let $f_i : \Sigma \dashrightarrow \Sigma$ for every $i \in \mathbb{N}$ be given by
$$f_i(\sigma) := \begin{cases} \sigma[x \mapsto \sigma(x) + 1] & \text{if } \sigma(x) \leq i \\ \text{undefined} & \text{otherwise} \end{cases}$$
Then $S := \{f_0, f_1, f_2, \ldots\}$ is a chain (Example 6.5(3)) with $\bigsqcup S = f$ where
$$f : \Sigma \to \Sigma : \sigma \mapsto \sigma[x \mapsto \sigma(x) + 1]$$