

AAA616: Program Analysis

Lecture 10 — Denotational Semantics

Hakjoo Oh
2026 Fall

Denotational Semantics

- In denotational semantics, we are interested in the mathematical meaning of a program.
- Also called compositional semantics: The meaning of an expression is defined with the meanings of its immediate subexpressions.
- Denotational semantics for **While**:

$$a \rightarrow n \mid x \mid a_1 + a_2 \mid a_1 \star a_2 \mid a_1 - a_2$$
$$b \rightarrow \text{true} \mid \text{false} \mid a_1 = a_2 \mid a_1 \leq a_2 \mid \neg b \mid b_1 \wedge b_2$$
$$c \rightarrow x := a \mid \text{skip} \mid c_1; c_2 \mid \text{if } b \text{ } c_1 \text{ } c_2 \mid \text{while } b \text{ } c$$

Denotational Semantics of Expressions

$$\mathcal{A}[[a]] \quad : \quad \mathbf{State} \rightarrow \mathbb{Z}$$

$$\mathcal{A}[[n]](s) = n$$

$$\mathcal{A}[[x]](s) = s(x)$$

$$\mathcal{A}[[a_1 + a_2]](s) = \mathcal{A}[[a_1]](s) + \mathcal{A}[[a_2]](s)$$

$$\mathcal{A}[[a_1 \star a_2]](s) = \mathcal{A}[[a_1]](s) \times \mathcal{A}[[a_2]](s)$$

$$\mathcal{A}[[a_1 - a_2]](s) = \mathcal{A}[[a_1]](s) - \mathcal{A}[[a_2]](s)$$

$$\mathcal{B}[[b]] \quad : \quad \mathbf{State} \rightarrow \mathbf{T}$$

$$\mathcal{B}[[\text{true}]](s) = \text{true}$$

$$\mathcal{B}[[\text{false}]](s) = \text{false}$$

$$\mathcal{B}[[a_1 = a_2]](s) = \mathcal{A}[[a_1]](s) = \mathcal{A}[[a_2]](s)$$

$$\mathcal{B}[[a_1 \leq a_2]](s) = \mathcal{A}[[a_1]](s) \leq \mathcal{A}[[a_2]](s)$$

$$\mathcal{B}[[\neg b]](s) = \mathcal{B}[[b]](s) = \text{false}$$

$$\mathcal{B}[[b_1 \wedge b_2]](s) = \mathcal{B}[[b_1]](s) \wedge \mathcal{B}[[b_2]](s)$$

Denotational Semantics of Commands

$$\begin{aligned}\mathcal{C}[[c]] &: \mathbf{State} \hookrightarrow \mathbf{State} \\ \mathcal{C}[[x := a]](s) &= s[x \mapsto \mathcal{A}[[a]](s)] \\ \mathcal{C}[[\text{skip}]] &= \text{id} \\ \mathcal{C}[[c_1; c_2]] &= \mathcal{C}[[c_2]] \circ \mathcal{C}[[c_1]] \\ \mathcal{C}[[\text{if } b \text{ } c_1 \text{ } c_2]] &= \text{cond}(\mathcal{B}[[b]], \mathcal{C}[[c_1]], \mathcal{C}[[c_2]]) \\ \mathcal{C}[[\text{while } b \text{ } c]] &= \text{fix } F\end{aligned}$$

where

$$\text{cond}(f, g, h) = \lambda s. \begin{cases} g(s) & \cdots f(s) = \text{true} \\ h(s) & \cdots f(s) = \text{false} \end{cases}$$

$$F(g) = \text{cond}(\mathcal{B}[[b]], g \circ \mathcal{C}[[c]], \text{id})$$

Denotational Semantics of Loops

The meaning of the while loop is the mathematical object (i.e. partial function in **State** $\hookrightarrow$ **State**) that satisfies the equation:

$$\mathcal{C}[\text{while } b \text{ } c] = \text{cond}(\mathcal{B}[b], \mathcal{C}[\text{while } b \text{ } c] \circ \mathcal{C}[c], \text{id}).$$

Rewrite the equation:

$$\mathcal{C}[\text{while } b \text{ } c] = F(\mathcal{C}[\text{while } b \text{ } c])$$

where

$$F(g) = \text{cond}(\mathcal{B}[b], g \circ \mathcal{C}[c], \text{id}).$$

The meaning of the while loop is defined as the least fixed point of F :

$$\mathcal{C}[\text{while } b \text{ } c] = \text{fix } F$$

where $\text{fix } F$ denotes the *least fixed point* of F .

Example

`while  $\neg(x = 0)$  skip`

- F
- $fix F$

Questions

- Does the least fixed point $\text{fix } F$ exist?
- Is $\text{fix } F$ unique?
- How to compute $\text{fix } F$?

Fixed Point Theory

Theorem

Let $f : D \rightarrow D$ be a continuous function on a CPO D . Then f has a (unique) least fixed point, $\text{fix}(f)$, and

$$\text{fix}(f) = \bigsqcup_{n \geq 0} f^n(\perp).$$

The denotational semantics is well-defined if

- **State** $\hookrightarrow$ **State** is a CPO, and
- $F : (\text{State} \hookrightarrow \text{State}) \rightarrow (\text{State} \hookrightarrow \text{State})$ is a continuous function.

Plan

- Complete Partial Order
- Continuous Functions
- Least Fixed Point

Partially Ordered Set

Definition (Partial Order)

We say a binary relation $\sqsubseteq$ is a partial order on a set D iff $\sqsubseteq$ is

- reflexive: $\forall p \in D. p \sqsubseteq p$
- transitive: $\forall p, q, r \in D. p \sqsubseteq q \wedge q \sqsubseteq r \implies p \sqsubseteq r$
- anti-symmetric: $\forall p, q \in D. p \sqsubseteq q \wedge q \sqsubseteq p \implies p = q$

We call such a pair $(D, \sqsubseteq)$ partially ordered set, or poset.

Lemma

If a partially ordered set $(D, \sqsubseteq)$ has a least element d , then d is unique.

Exercise 1

Let S be a non-empty set. Prove that $(\wp(S), \subseteq)$ is a partially ordered set.

Exercise 2

Let $X \hookrightarrow Y$ be the set of all partial functions from a set X to a set Y , and define $f \sqsubseteq g$ iff

$$\mathbf{dom}(f) \subseteq \mathbf{dom}(g) \wedge \forall x \in \mathbf{dom}(f). f(x) = g(x).$$

Prove that $(X \hookrightarrow Y, \sqsubseteq)$ is a partially ordered set.

Least Upper Bound

Definition (Least Upper Bound)

Let $(D, \sqsubseteq)$ be a partially ordered set and let Y be a subset of D . An upper bound of Y is an element d of D such that

$$\forall d' \in Y. d' \sqsubseteq d.$$

An upper bound d of Y is a least upper bound if and only if $d \sqsubseteq d'$ for every upper bound d' of Y . The least upper bound of Y is denoted by $\sqcup Y$. The least upper bound (lub, join) of a and b is written as $a \sqcup b$.

Lemma

If Y has a least upper bound d , then d is unique.

Greatest Lower Bound

Definition (Greatest Lower Bound)

Let $(D, \sqsubseteq)$ be a partially ordered set and let Y be a subset of D . A lower bound of Y is an element d of D such that

$$\forall d' \in Y. d \sqsubseteq d'.$$

An lower bound d of Y is a greatest lower bound if and only if $d' \sqsubseteq d$ for every lower bound d' of Y . The greatest lower bound of Y is denoted by $\sqcap Y$. The greatest lower bound (glb, meet) of a and b is written as $a \sqcap b$.

Chain

Definition (Chain)

Let $(D, \sqsubseteq)$ be a poset and Y a subset of D . Y is called a chain if Y is totally ordered:

$$\forall y_1, y_2 \in Y. y_1 \sqsubseteq y_2 \text{ or } y_2 \sqsubseteq y_1.$$

Example

Consider the poset $(\wp(\{a, b, c\}), \subseteq)$.

- $Y_1 = \{\emptyset, \{a\}, \{a, c\}\}$
- $Y_2 = \{\emptyset, \{a\}, \{c\}, \{a, c\}\}$

Complete Partial Order (CPO)

Definition (CPO)

A poset $(D, \sqsubseteq)$ is a CPO, if every chain $Y \subseteq D$ has $\bigsqcup Y \in D$.

Lemma

If $(D, \sqsubseteq)$ is a CPO, then it has a least element $\perp$ given by $\perp = \bigsqcup \emptyset$.

* We denote the least element and the greatest element in a poset as $\perp$ and $\top$, respectively, if they exist.

Examples

Example

Let S be a non-empty set. Then, $(\wp(S), \subseteq)$ is a CPO. The lub $\bigsqcup Y$ for Y is $\bigcup Y$. The least element is $\emptyset$.

Examples

Example

The poset $(X \hookrightarrow Y, \sqsubseteq)$ of all partial functions from a set X to a set Y , equipped with the partial order

$$\mathbf{dom}(f) \subseteq \mathbf{dom}(g) \wedge \forall x \in \mathbf{dom}(f). f(x) = g(x)$$

is a CPO (but not a complete lattice). The lub of a chain Y is the partial function f with $\mathbf{dom}(f) = \bigcup_{f_i \in Y} \mathbf{dom}(f_i)$ and

$$f(x) = \begin{cases} f_n(x) & \dots x \in \mathbf{dom}(f_i) \text{ for some } f_i \in Y \\ \dots otherwise \end{cases}$$

The least element $\perp = \lambda x.\mathbf{undef}$.

Lattices

Ordered sets with richer structures.

Definition (Lattice)

A lattice $(D, \sqsubseteq, \sqcup, \sqcap)$ is a poset where the lub and glb always exist:

$$\forall a, b \in D. a \sqcup b \in D \wedge a \sqcap b \in D.$$

Definition (Complete Lattice)

A complete lattice $(D, \sqsubseteq, \sqcup, \sqcap, \perp, \top)$ is a poset such that every subset $Y \subseteq D$ has $\bigsqcup Y \in D$ and $\bigsqcap Y \in D$, and D has a least element $\perp = \bigsqcup \emptyset = \bigsqcap D$ and a greatest element $\top = \bigsqcap \emptyset = \bigsqcup D$.

* A complete lattice is a CPO.

Derived Ordered Structures

When $(D_1, \sqsubseteq_1, \sqcup_1, \sqcap_1, \perp_1, \top_1)$ and $(D_2, \sqsubseteq_2, \sqcup_2, \sqcap_2, \perp_2, \top_2)$ are complete lattices (resp., CPO), so are the following ordered sets:

- Lifting: $(D_1 \cup \{\perp\}, \sqsubseteq, \sqcup, \sqcap, \perp, \top)$
 - ▶ $\perp \notin D_1$ is a new element
 - ▶ $a \sqsubseteq b \iff a = \perp \vee a \sqsubseteq_1 b$
 - ▶ $\perp \sqcup a = a \sqcup \perp = a$ and otherwise $a \sqcup b = a \sqcup_1 b$ (similar for $\sqcap$)
 - ▶ $\top = \top_1$
- Cartesian product: $(D_1 \times D_2, \sqsubseteq, \sqcup, \sqcap, \perp, \top)$.
- Pointwise lifting: $(S \rightarrow D, \sqsubseteq, \sqcup, \sqcap, \perp, \top)$ (S is a set)
 - ▶ $a \sqsubseteq b \iff \forall s \in S. a(s) \sqsubseteq_1 b(s)$
 - ▶ $\forall s \in S. (a \sqcup b)(s) \iff a(s) \sqcup_1 b(s)$
 - ▶ $\forall s \in S. \perp(s) = \perp_1$

Monotone Functions

Definition (Monotone Functions)

A function $f : D \rightarrow E$ between posets is *monotone* iff

$$\forall d, d' \in D. d \sqsubseteq d' \implies f(d) \sqsubseteq f(d').$$

Example

Consider $(\wp(\{a, b, c\}), \subseteq)$ and $(\wp(\{d, e\}), \subseteq)$ and two functions $f_1, f_2 : \wp(\{a, b, c\}) \rightarrow \wp(\{d, e\})$

X	$\{a, b, c\}$	$\{a, b\}$	$\{a, c\}$	$\{b, c\}$	$\{a\}$	$\{b\}$	$\{c\}$	$\emptyset$
$f_1(X)$	$\{d, e\}$	$\{d\}$	$\{d, e\}$	$\{d, e\}$	$\{d\}$	$\{d\}$	$\{e\}$	$\emptyset$

X	$\{a, b, c\}$	$\{a, b\}$	$\{a, c\}$	$\{b, c\}$	$\{a\}$	$\{b\}$	$\{c\}$	$\emptyset$
$f_2(X)$	$\{d\}$	$\{d\}$	$\{d\}$	$\{e\}$	$\{d\}$	$\{e\}$	$\{e\}$	$\{e\}$

Exercise

Determine which of the following functionals of

$$(\mathbf{State} \hookrightarrow \mathbf{State}) \rightarrow (\mathbf{State} \hookrightarrow \mathbf{State})$$

are monotone:

$$\textcircled{1} \quad F_0(g) = g.$$

$$\textcircled{2} \quad F_1(g) = \begin{cases} g_1 & \dots g = g_2 \\ g_2 & \dots otherwise \end{cases} \quad \text{where } g_1 \neq g_2.$$

$$\textcircled{3} \quad F_2(g) = \lambda s. \begin{cases} g(s) & \dots s(x) \neq 0 \\ s & \dots s(x) = 0 \end{cases}$$

Properties of Monotone Functions

Lemma

Let $(D_1, \sqsubseteq_1)$, $(D_2, \sqsubseteq_2)$, and $(D_3, \sqsubseteq_3)$ be CPOs. Let $f : D_1 \rightarrow D_2$ and $g : D_2 \rightarrow D_3$ be monotone functions. Then, $g \circ f : D_1 \rightarrow D_3$ is a monotone function.

Properties of Monotone Functions

Lemma

Let $(D_1, \sqsubseteq_1)$ and $(D_2, \sqsubseteq_2)$ be CPOs. Let $f : D_1 \rightarrow D_2$ be a monotone function. If Y is a chain in D_1 , then $f(Y) = \{f(d) \mid d \in Y\}$ is a chain in D_2 . Furthermore,

$$\bigsqcup f(Y) \sqsubseteq f(\bigsqcup Y).$$

Continuous Functions

Definition (Continuous Functions)

A function $f : D_1 \rightarrow D_2$ defined on CPOs $(D_1, \sqsubseteq_1)$ and $(D_2, \sqsubseteq_2)$ is continuous if it is monotone and it preserves least upper bounds of chains:

$$\bigsqcup f(Y) = f(\bigsqcup Y)$$

for all non-empty chains Y in D_1 . If $f(\bigsqcup Y) = \bigsqcup f(Y)$ holds for the empty chain (that is, $\perp = f(\perp)$), then we say that f is strict.

Properties of Continuous Functions

Lemma

Let $f : D_1 \rightarrow D_2$ be a monotone function defined on posets $(D_1, \sqsubseteq_1)$ and $(D_2, \sqsubseteq_2)$ and D_1 is a finite set. Then, f is continuous.

Properties of Continuous Functions

Lemma

Let $(D_1, \sqsubseteq_1)$, $(D_2, \sqsubseteq_2)$, and $(D_3, \sqsubseteq_3)$ be CPOs. Let $f : D_1 \rightarrow D_2$ and $g : D_2 \rightarrow D_3$ be continuous functions. Then, $g \circ f : D_1 \rightarrow D_3$ is a continuous function.

Least Fixed Points

Definition (Fixed Point)

Let $(D, \sqsubseteq)$ be a poset. A *fixed point* of a function $f : D \rightarrow D$ is an element $d \in D$ such that $f(d) = d$. We write $\text{fix}(f)$ for the *least fixed point* of f , if it exists, such that

- $f(\text{fix}(f)) = \text{fix}(f)$
- $\forall d \in D. f(d) = d \implies \text{fix}(f) \sqsubseteq d$

* More notations:

- x is a fixed point of f if $f(x) = x$. Let $\mathbf{fp}(f) = \{x \mid f(x) = x\}$ be the set of fixed points.
- x is a pre-fixed point of f if $x \sqsubseteq f(x)$.
- x is a post-fixed point of f if $x \sqsupseteq f(x)$.
- $\mathbf{lfp}(f)$: the least fixed point
- $\mathbf{gfp}(f)$: the greatest fixed point

Fixed Point Theorem

Theorem (Kleene Fixed Point)

Let $f : D \rightarrow D$ be a continuous function on a CPO D . Then f has a least fixed point, $\text{fix}(f)$, and

$$\text{fix}(f) = \bigsqcup_{n \geq 0} f^n(\perp)$$

$$\text{where } f^n(\perp) = \begin{cases} \perp & n = 0 \\ f(f^{n-1}(\perp)) & n > 0 \end{cases}$$

Proof

We show the claims of the theorem by showing that $\bigsqcup_{n \geq 0} f^n(\perp)$ exists and it is indeed equivalent to $\text{fix}(f)$. First note that $\bigsqcup_{n \geq 0} f^n(\perp)$ exists because $f^0(\perp) \sqsubseteq f^1(\perp) \sqsubseteq f^2(\perp) \sqsubseteq \dots$ is a chain. We show by induction that $\forall n \in \mathbb{N}. f^n(\perp) \sqsubseteq f^{n+1}(\perp)$:

- $\perp \sqsubseteq f(\perp)$ ($\perp$ is the least element)
- $f^n(\perp) \sqsubseteq f^{n+1}(\perp) \implies f^{n+1}(\perp) \sqsubseteq f^{n+2}(\perp)$ (monotonicity of f)

Now, we show that $\text{fix}(f) = \bigsqcup_{n \geq 0} f^n(\perp)$ in two steps:

- We show that $\bigsqcup_{n \geq 0} f^n(\perp)$ is a fixed point of f :

$$\begin{aligned} f\left(\bigsqcup_{n \geq 0} f^n(\perp)\right) &= \bigsqcup_{n \geq 0} f(f^n(\perp)) && \text{continuity of } f \\ &= \bigsqcup_{n \geq 0} f^{n+1}(\perp) \\ &= \bigsqcup_{n \geq 0} f^n(\perp) \end{aligned}$$

Proofs

- We show that $\bigsqcup_{n \geq 0} f^n(\perp)$ is smaller than all the other fixed points. Suppose d is a fixed point, i.e., $f(d) = d$. Then,

$$\bigsqcup_{n \geq 0} f^n(\perp) \sqsubseteq d$$

since $\forall n \in \mathbb{N}. f^n(\perp) \sqsubseteq d$:

$$f^0(\perp) = \perp \sqsubseteq d, \quad f^n(\perp) \sqsubseteq d \implies f^{n+1}(\perp) \sqsubseteq f(d) = d.$$

Therefore, we conclude

$$fix(f) = \bigsqcup_{n \geq 0} f^n(\perp).$$

Well-definedness of the Semantics

The function F

$$F(g) = \text{cond}(\mathcal{B}[[b]], g \circ \mathcal{C}[[c]], \text{id})$$

is continuous.

Lemma

Let $g_0 : \text{State} \hookrightarrow \text{State}$, $p : \text{State} \rightarrow \mathbf{T}$, and define

$$F(g) = \text{cond}(p, g, g_0).$$

Then, F is continuous.

Lemma

Let $g_0 : \text{State} \hookrightarrow \text{State}$, and define

$$F(g) = g \circ g_0.$$

Then F is continuous.