Lecture 6 – Fixed-Point Theory

AAA551: Programming Language Theory

Jihyeok Park

PLRG

2026 Spring

Recall

- Denotational Semantics
- Simple Imperative Language – IMP
  - Expressions
  - Statements
  - Solving Recursive Equations
  - `while` Statement Revisited
  - Explicit Errors
- Non-Deterministic Imperative Language – NIMP
  - Expressions
  - Statements

`while` Statement

$$S[\![\texttt{while } e \texttt{ do } s]\!] \triangleq \mathbf{lfp}(F) = \bigcup_{n \in \mathbb{Z}} F^n(\varnothing)$$

where

$$F(f)(\sigma) = \begin{cases} \sigma & \text{if } E[\![e]\!](\sigma) = \texttt{false} \\ f(S[\![s]\!](\sigma)) & \text{if } E[\![e]\!](\sigma) = \texttt{true} \\ \text{undefined} & \text{otherwise} \end{cases}$$

Contents

Contents

Partial Orders

Definition (Partial Orders)

A *partial order* is a binary relation $\sqsubseteq$ on a set S that is:

- **reflexive**: $\forall x \in S, x \sqsubseteq x$
- **antisymmetric**: $\forall x, y \in S, (x \sqsubseteq y \land y \sqsubseteq x) \implies x = y$
- **transitive**: $\forall x, y, z \in S, (x \sqsubseteq y \land y \sqsubseteq z) \implies x \sqsubseteq z$.

We call the pair $(S, \sqsubseteq)$ a *partially ordered set* (or *poset*).

We use the notation $x \sqsubset y \triangleq (x \sqsubseteq y \land x \neq y)$.

Partial Orders

PLRG

Definition (Partial Orders)

A *partial order* is a binary relation $\sqsubseteq$ on a set S that is:

- **reflexive**: $\forall x \in S, x \sqsubseteq x$
- **antisymmetric**: $\forall x, y \in S, (x \sqsubseteq y \land y \sqsubseteq x) \implies x = y$
- **transitive**: $\forall x, y, z \in S, (x \sqsubseteq y \land y \sqsubseteq z) \implies x \sqsubseteq z$.

We call the pair $(S, \sqsubseteq)$ a *partially ordered set* (or *poset*).

We use the notation $x \sqsubset y \triangleq (x \sqsubseteq y \land x \neq y)$.

Example

$(\mathcal{P}(X), \subseteq)$ is a poset for any set X.

- **reflexive**: $\forall A \subseteq \mathbb{Z}, A \subseteq A$
- **antisymmetric**: $\forall A, B \subseteq \mathbb{Z}, (A \subseteq B \land B \subseteq A) \implies A = B$
- **transitive**: $\forall A, B, C \subseteq \mathbb{Z}, (A \subseteq B \land B \subseteq C) \implies A \subseteq C$

Partial Orders – Hasse Diagrams

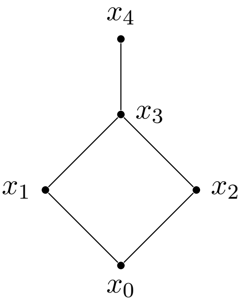
We often use *Hasse diagrams* to visually represent posets.

A poset $(S, \sqsubseteq)$ is defined as follows:

- $S \triangleq \{x_0, x_1, x_2, x_3, x_4\}$
- $\sqsubseteq$ is the smallest partial order on S such that:

$$x_0 \sqsubseteq x_1$$
$$x_0 \sqsubseteq x_2$$
$$x_1 \sqsubseteq x_3$$
$$x_2 \sqsubseteq x_3$$
$$x_3 \sqsubseteq x_4$$

Hasse diagram of $(S, \sqsubseteq)$:



By definition of reflexivity, $x_i \sqsubseteq x_i$ for all $0 \leq i \leq 4$.

By definition of transitivity,

- $x_0 \sqsubseteq x_3 \qquad (\because x_0 \sqsubseteq x_1 \sqsubseteq x_3)$
- $x_2 \sqsubseteq x_4 \qquad (\because x_2 \sqsubseteq x_3 \sqsubseteq x_4)$

Total Orders

Definition (Total Orders)

A *total order* is a partial order $\sqsubseteq$ on a set S such that:

- **total**: $\forall x, y \in S, (x \sqsubseteq y \vee y \sqsubseteq x)$

Total Orders

PLRG

Definition (Total Orders)

A *total order* is a partial order $\sqsubseteq$ on a set S such that:

- **total**: $\forall x, y \in S, (x \sqsubseteq y \vee y \sqsubseteq x)$

Example

$(\mathbb{Z}, \leq)$ is a total order.

- **reflexive**: $\forall n \in \mathbb{Z}, n \leq n$
- **antisymmetric**: $\forall m, n \in \mathbb{Z}, (m \leq n \wedge n \leq m) \implies m = n$
- **transitive**: $\forall m, n, p \in \mathbb{Z}, (m \leq n \wedge n \leq p) \implies m \leq p$
- **total**: $\forall m, n \in \mathbb{Z}, (m \leq n \vee n \leq m)$

Total Orders

Definition (Total Orders)

A *total order* is a partial order $\sqsubseteq$ on a set S such that:

- **total**: $\forall x, y \in S, (x \sqsubseteq y \vee y \sqsubseteq x)$

Example

$(\mathbb{Z}, \leq)$ is a total order.

- **reflexive**: $\forall n \in \mathbb{Z}, n \leq n$
- **antisymmetric**: $\forall m, n \in \mathbb{Z}, (m \leq n \wedge n \leq m) \implies m = n$
- **transitive**: $\forall m, n, p \in \mathbb{Z}, (m \leq n \wedge n \leq p) \implies m \leq p$
- **total**: $\forall m, n \in \mathbb{Z}, (m \leq n \vee n \leq m)$

Example

$(\mathcal{P}(S), \sqsubseteq)$ is a poset but not total.

- $\{x\}$ and $\{y\}$ are incomparable if $x \neq y$ and $x, y \in S$.

Minimum and Maximum Elements

Definition (Minimum and Maximum Elements)

Let $(S, \sqsubseteq)$ be a poset and $x \in S$. Then, x is:

- the *maximum element* of S if $\forall y \in S, y \sqsubseteq x$
- the *minimum element* of S if $\forall y \in S, x \sqsubseteq y$

Minimum and Maximum Elements

Definition (Minimum and Maximum Elements)

Let $(S, \sqsubseteq)$ be a poset and $x \in S$. Then, x is:

- the *maximum element* of S if $\forall y \in S, y \sqsubseteq x$
- the *minimum element* of S if $\forall y \in S, x \sqsubseteq y$

We often use the following notations:

- $\top$ (**"top"**) to denote the maximum element
- $\bot$ (**"bottom"**) to denote the minimum element

Minimum and Maximum Elements

Definition (Minimum and Maximum Elements)

Let $(S, \sqsubseteq)$ be a poset and $x \in S$. Then, x is:

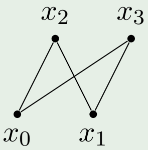
- the *maximum element* of S if $\forall y \in S, y \sqsubseteq x$
- the *minimum element* of S if $\forall y \in S, x \sqsubseteq y$

We often use the following notations:

- $\top$ (**"top"**) to denote the maximum element
- $\bot$ (**"bottom"**) to denote the minimum element

Example

The following poset does not have the minimum or maximum element.



Bounds

Definition (Bounds)

Let $(S, \sqsubseteq)$ be a poset and $T \subseteq S$. Then, $x \in S$ is:

- an *upper bound* of T if:

$$\forall t \in T, t \sqsubseteq x$$

- the *least upper bound* (lub or **join**) of T if:

$$\forall t \in T, t \sqsubseteq x \land \forall y \in S, (\forall t \in T, t \sqsubseteq y) \implies x \sqsubseteq y$$

Dually, we define *lower bounds* and *greatest lower bounds* (glb or **meet**).

Bounds

Definition (Bounds)

Let $(S, \sqsubseteq)$ be a poset and $T \subseteq S$. Then, $x \in S$ is:

- an *upper bound* of T if:

$$\forall t \in T, t \sqsubseteq x$$

- the *least upper bound* (lub or **join**) of T if:

$$\forall t \in T, t \sqsubseteq x \land \forall y \in S, (\forall t \in T, t \sqsubseteq y) \implies x \sqsubseteq y$$

Dually, we define *lower bounds* and *greatest lower bounds* (glb or **meet**).

Not all subsets have lubs or glbs.

If T has the lub (or glb), it is unique and we denote it as $\bigsqcup T$ (or $\bigsqcap T$).

Bounds

PLRG

Definition (Bounds)

Let $(S, \sqsubseteq)$ be a poset and $T \subseteq S$. Then, $x \in S$ is:

- an *upper bound* of T if:

$$\forall t \in T, t \sqsubseteq x$$

- the *least upper bound* (lub or **join**) of T if:

$$\forall t \in T, t \sqsubseteq x \wedge \forall y \in S, (\forall t \in T, t \sqsubseteq y) \implies x \sqsubseteq y$$

Dually, we define *lower bounds* and *greatest lower bounds* (glb or **meet**).

Not all subsets have lubs or glbs.

If T has the lub (or glb), it is unique and we denote it as $\bigsqcup T$ (or $\bigsqcap T$).

We use the notations $x \sqcup y \triangleq \bigsqcup\{x, y\}$ and $x \sqcap y \triangleq \bigsqcap\{x, y\}$.

Chains

Definition (Chains)

Let $(S, \sqsubseteq)$ be a poset. A subset $C \subseteq S$ is a *chain* if $(C, \sqsubseteq)$ is a total, i.e.,

$$\forall x, y \in C, (x \sqsubseteq y \vee y \sqsubseteq x)$$

Chains

Definition (Chains)

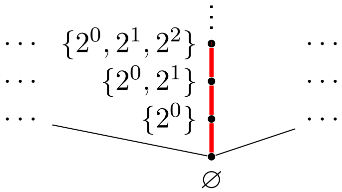
Let $(S, \sqsubseteq)$ be a poset. A subset $C \subseteq S$ is a *chain* if $(C, \sqsubseteq)$ is a total, i.e.,

$$\forall x, y \in C, (x \sqsubseteq y \vee y \sqsubseteq x)$$

Example

In the poset $(\mathcal{P}(\mathbb{N}), \subseteq)$, the following subset $C \subseteq \mathcal{P}(\mathbb{N})$ is an infinite chain:

$$C = \{c_i \mid i \in \mathbb{N}\} \text{ where } \forall i \in \mathbb{N}, c_i = \{2^j \mid 0 \leq j < i\}$$



Complete Partial Orders

Definition (Complete Partial Orders)

A *complete partial order* (CPO) is a poset $(S, \sqsubseteq)$ if every chain $C \subseteq S$ has the lub $\bigsqcup C$.

Complete Partial Orders

Definition (Complete Partial Orders)

A *complete partial order* (CPO) is a poset $(S, \sqsubseteq)$ if every chain $C \subseteq S$ has the lub $\bigsqcup C$.

Lemma

Let $(S, \sqsubseteq)$ be a CPO. Then, S has the minimum element $\bot$.

Complete Partial Orders

PLRG

Definition (Complete Partial Orders)

A *complete partial order* (CPO) is a poset $(S, \sqsubseteq)$ if every chain $C \subseteq S$ has the lub $\bigsqcup C$.

Lemma

Let $(S, \sqsubseteq)$ *be a CPO. Then,* S *has the minimum element* $\bot$*.*

The empty set $\varnothing$ is a chain because it is vacuously total.

Since the lub of $\varnothing$ is the minimum element $\bot$ (i.e., $\bigsqcup \varnothing = \bot$), S has the minimum element $\bot$.

Lattices

PLRG

Definition (Lattices)

A *lattice* $(S, \sqsubseteq, \sqcup, \sqcap)$ is a poset such that:

$$\forall x, y \in S, x \sqcup y \text{ and } x \sqcap y \text{ exist in } S$$

All finite subsets $T \subseteq S$ have lubs and glbs because we can compute them by iteratively applying $\sqcup$ and $\sqcap$ to the elements of T.

Lattices

Definition (Lattices)

A *lattice* $(S, \sqsubseteq, \sqcup, \sqcap)$ is a poset such that:

$$\forall x, y \in S, x \sqcup y \text{ and } x \sqcap y \text{ exist in } S$$

All finite subsets $T \subseteq S$ have lubs and glbs because we can compute them by iteratively applying $\sqcup$ and $\sqcap$ to the elements of T.

Definition (Complete Lattices)

A *complete lattice* $(S, \sqsubseteq, \sqcup, \sqcap, \top, \bot)$ is a poset such that:

$$\forall T \subseteq S, \bigsqcup T \text{ and } \bigsqcap T \text{ exist in } S$$

Every complete lattice:

- has the **maximum** $\top = \bigsqcup S = \bigsqcap \varnothing$ and **minimum** $\bot = \bigsqcap S = \bigsqcup \varnothing$.
- is **lattice** because every pair is a subset.
- is a **CPO** because every chain is a subset.

Posets vs. CPOs and Posets vs. Lattices

Not all posets are CPOs or lattices.

Example

$(\mathbb{N}, \leq_2)$ is a poset where $\leq_2$ is defined as follows:

$$\forall x, y \in \mathbb{N}. \quad x \leq_2 y \quad \triangleq \quad (x \leq y) \land (x \equiv y \pmod 2)$$

but it is neither a CPO nor a lattice.

Posets vs. CPOs and Posets vs. Lattices

Not all posets are CPOs or lattices.

Example

$(\mathbb{N}, \leq_2)$ is a poset where $\leq_2$ is defined as follows:

$$\forall x, y \in \mathbb{N}. \quad x \leq_2 y \quad \triangleq \quad (x \leq y) \land (x \equiv y \pmod 2)$$

but it is neither a CPO nor a lattice.

It is not a CPO:

- $C = \{0, 2, 4, \dots\}$ is a chain because it is a total order.
- C does not have the lub in $\mathbb{N}$.

Posets vs. CPOs and Posets vs. Lattices

Not all posets are CPOs or lattices.

Example

$(\mathbb{N}, \leq_2)$ is a poset where $\leq_2$ is defined as follows:

$$\forall x, y \in \mathbb{N}. \quad x \leq_2 y \quad \triangleq \quad (x \leq y) \land (x \equiv y \pmod 2)$$

but it is neither a CPO nor a lattice.

It is not a CPO:

- $C = \{0, 2, 4, \dots\}$ is a chain because it is a total order.
- C does not have the lub in $\mathbb{N}$.

It is not a lattice:

- 0 and 1 do not have the lub in $\mathbb{N}$.
- 0 and 1 do not have the glb in $\mathbb{N}$.

CPOs vs. Lattices

PLRG

Not all CPOs are lattices.

Example

$(X \rightharpoonup Y, \sqsubseteq)$ for *partial functions* from X to Y is a CPO where $f \sqsubseteq g$ if:

$$\mathsf{dom}(f) \subseteq \mathsf{dom}(g) \quad \land \quad \forall x \in \mathsf{dom}(f), f(x) = g(x)$$

for all $f, g \in X \rightharpoonup Y$, but it is not a lattice.

The minimum element $\bot$ is the empty function $\varnothing$.

CPOs vs. Lattices

Not all CPOs are lattices.

Example

$(X \rightharpoonup Y, \sqsubseteq)$ for *partial functions* from X to Y is a CPO where $f \sqsubseteq g$ if:

$$\mathsf{dom}(f) \subseteq \mathsf{dom}(g) \quad \land \quad \forall x \in \mathsf{dom}(f), f(x) = g(x)$$

for all $f, g \in X \rightharpoonup Y$, but it is not a lattice.

The minimum element $\bot$ is the empty function $\varnothing$.

It is a CPO because we can define lub of any chain C as follows:

$$(\bigsqcup C)(x) = \begin{cases} f(x) & \text{if } \exists f \in C.\ x \in \mathsf{dom}(f) \\ \text{undefined} & \text{otherwise} \end{cases}$$

CPOs vs. Lattices

Not all CPOs are lattices.

Example

$(X \rightharpoonup Y, \sqsubseteq)$ for *partial functions* from X to Y is a CPO where $f \sqsubseteq g$ if:

$$\mathsf{dom}(f) \subseteq \mathsf{dom}(g) \quad \land \quad \forall x \in \mathsf{dom}(f), f(x) = g(x)$$

for all $f, g \in X \rightharpoonup Y$, but it is not a lattice.

The minimum element $\bot$ is the empty function $\varnothing$.

It is a CPO because we can define lub of any chain C as follows:

$$(\bigsqcup C)(x) = \begin{cases} f(x) & \text{if } \exists f \in C.\ x \in \mathsf{dom}(f) \\ \text{undefined} & \text{otherwise} \end{cases}$$

It is not a lattice because f and g do not have lub in $X \rightharpoonup Y$:

$$f = \{(x, y)\} \quad \text{and} \quad g = \{(x, y')\}$$

where $x \in X$ and $y, y' \in Y$ such that $y \neq y'$.

Lattices vs. CPOs

Not all lattices are CPOs.

Example

$(\mathbb{Z}^+, |)$ is a lattice where $|$ is the divisibility relation defined as:

$$\forall m, n \in \mathbb{Z}^+. \quad m \mid n \quad \triangleq \quad \exists k \in \mathbb{Z}^+. \, n = m \cdot k$$

but it is not a CPO.

The minimum element $\bot$ is 1 because $1 \mid n$ for all $n \in \mathbb{Z}^+$.

Lattices vs. CPOs

Not all lattices are CPOs.

Example

$(\mathbb{Z}^+, |)$ is a lattice where $|$ is the divisibility relation defined as:

$$\forall m, n \in \mathbb{Z}^+. \quad m \mid n \quad \triangleq \quad \exists k \in \mathbb{Z}^+.\, n = m \cdot k$$

but it is not a CPO.

The minimum element $\bot$ is 1 because $1 \mid n$ for all $n \in \mathbb{Z}^+$.

It is a lattice because we can define:

- $m \sqcup n = \mathrm{lcm}(m, n)$ (least common multiple)
- $m \sqcap n = \gcd(m, n)$ (greatest common divisor)

Lattices vs. CPOs

Not all lattices are CPOs.

Example

$(\mathbb{Z}^+, |)$ is a lattice where $|$ is the divisibility relation defined as:

$$\forall m, n \in \mathbb{Z}^+. \quad m \mid n \quad \triangleq \quad \exists k \in \mathbb{Z}^+.\ n = m \cdot k$$

but it is not a CPO.

The minimum element $\bot$ is 1 because $1 \mid n$ for all $n \in \mathbb{Z}^+$.

It is a lattice because we can define:

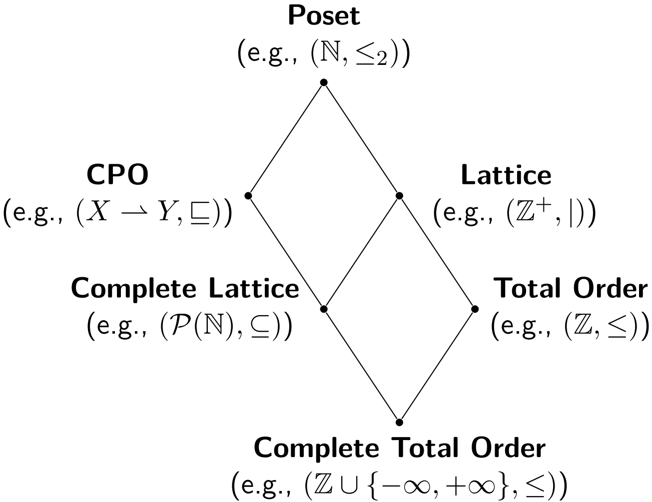
- $m \sqcup n = \mathrm{lcm}(m, n)$ (least common multiple)
- $m \sqcap n = \gcd(m, n)$ (greatest common divisor)

It is not a CPO because the following chain C does not have the lub in $\mathbb{Z}^+$:

$$C = \{2^i \mid i \in \mathbb{N}\}$$

Summary

The following Hasse diagram summarizes the implications between different classes of posets:



Contents

Monotone Functions

Definition (Monotone Functions)

Let $(S, \sqsubseteq)$ be a poset. A function $f : S \to S$ is *monotone* if:

$$\forall x, y \in S, x \sqsubseteq y \implies f(x) \sqsubseteq f(y)$$

$$\begin{array}{ccc} x & \xrightarrow{\quad f \quad} & f(x) \\ \text{\rotatebox{90}{$\sqsupseteq$}} & & \text{\rotatebox{90}{$\sqsupseteq$}} \\ y & \xrightarrow[\quad f \quad]{} & f(y) \end{array}$$

Monotone Functions

Definition (Monotone Functions)

Let $(S, \sqsubseteq)$ be a poset. A function $f : S \to S$ is *monotone* if:

$$\forall x, y \in S, x \sqsubseteq y \implies f(x) \sqsubseteq f(y)$$

$$\begin{array}{ccc} x & \xrightarrow{\quad f \quad} & f(x) \\ \rotatebox{90}{$\sqsupseteq$} & & \rotatebox{90}{$\sqsupseteq$} \\ y & \xrightarrow[\quad f \quad]{} & f(y) \end{array}$$

Example

Let $(\mathcal{P}(\mathbb{N}), \subseteq)$ be a poset. Then, the following functions are monotone:

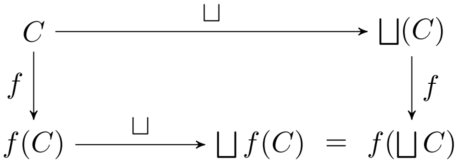
- $f(A) = A \cup \{42\}$
- $f(A) = A \cap S$ for some fixed $S \subseteq \mathbb{N}$

Continuous Functions

Definition (Continuous Functions)

Let $(S, \sqsubseteq)$ be a poset. A function $f : S \to S$ is (Scott) *continuous* if:

$$\forall C \subseteq S. \quad C \text{ is a non-empty chain} \implies f(\bigsqcup C) = \bigsqcup f(C)$$



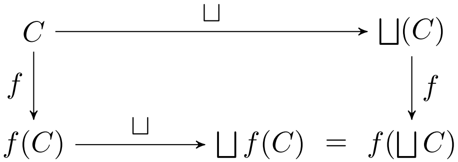
Continuous Functions

PLRG

Definition (Continuous Functions)

Let $(S, \sqsubseteq)$ be a poset. A function $f : S \to S$ is (Scott) *continuous* if:

$$\forall C \subseteq S. \quad C \text{ is a non-empty chain} \implies f(\bigsqcup C) = \bigsqcup f(C)$$



Example

Previously defined monotone functions on $(\mathcal{P}(\mathbb{N}), \subseteq)$ are also continuous, but the following function is not continuous:

$$f(A) = \begin{cases} \varnothing & \text{if } A \text{ is finite} \\ A & \text{otherwise} \end{cases}$$

Monotone vs. Continuous Functions

PLRG

Lemma

Function composition preserves monotonicity and continuity:

$$\forall f, g : S \to S. \quad \begin{cases} f \text{ and } g \text{ are monotone} \implies f \circ g \text{ is monotone} \\ f \text{ and } g \text{ are continuous} \implies f \circ g \text{ is continuous} \end{cases}$$

For all $x, y \in S$, $x \sqsubseteq y \implies g(x) \sqsubseteq g(y) \implies f(g(x)) \sqsubseteq f(g(y))$.

Similarly, for all non-empty chains $C \subseteq S$,

$$(f \circ g)(\bigsqcup C) = f(g(\bigsqcup C)) = f(\bigsqcup g(C)) = \bigsqcup f(g(C)) = \bigsqcup (f \circ g)(C)$$

Monotone vs. Continuous Functions

Lemma

Function composition preserves monotonicity and continuity:

$$\forall f, g : S \to S. \quad \begin{cases} f \text{ and } g \text{ are monotone} \implies f \circ g \text{ is monotone} \\ f \text{ and } g \text{ are continuous} \implies f \circ g \text{ is continuous} \end{cases}$$

For all $x, y \in S$, $x \sqsubseteq y \implies g(x) \sqsubseteq g(y) \implies f(g(x)) \sqsubseteq f(g(y))$.

Similarly, for all non-empty chains $C \subseteq S$,

$$(f \circ g)(\bigsqcup C) = f(g(\bigsqcup C)) = f(\bigsqcup g(C)) = \bigsqcup f(g(C)) = \bigsqcup (f \circ g)(C)$$

Lemma

Every continuous function $f : S \to S$ on a poset $(S, \sqsubseteq)$ is monotone.

Every pair $x, y \in S$ such that $x \sqsubseteq y$ forms a chain $\{x, y\}$.

Thus, $f(x) \sqsubseteq (f(x) \sqcup f(y)) = \bigsqcup f(\{x, y\}) = f(\bigsqcup \{x, y\}) = f(y)$.

Monotone vs. Continuous Functions

Lemma

In a monotone function $f : S \to S$ on a poset $(S, \sqsubseteq)$, if all chains are finite, then it is also continuous.

Let $C = c_0 \sqsubseteq c_1 \sqsubseteq \ldots \sqsubseteq c_n$ be a non-empty finite chain in S.

Then, $f(c_0) \sqsubseteq f(c_1) \sqsubseteq \ldots \sqsubseteq f(c_n)$ because f is monotone.

Thus, $f(\bigsqcup C) = f(c_n) = \bigsqcup f(C)$.

Monotone vs. Continuous Functions

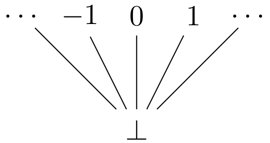
Lemma

In a monotone function $f : S \to S$ on a poset $(S, \sqsubseteq)$, if all chains are finite, then it is also continuous.

Let $C = c_0 \sqsubseteq c_1 \sqsubseteq \ldots \sqsubseteq c_n$ be a non-empty finite chain in S.

Then, $f(c_0) \sqsubseteq f(c_1) \sqsubseteq \ldots \sqsubseteq f(c_n)$ because f is monotone.

Thus, $f(\bigsqcup C) = f(c_n) = \bigsqcup f(C)$.



finite height

Monotone vs. Continuous Functions

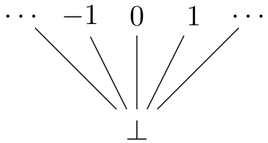
Lemma

In a monotone function $f : S \to S$ on a poset $(S, \sqsubseteq)$, if all chains are finite, then it is also continuous.

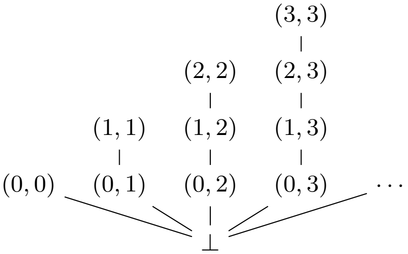
Let $C = c_0 \sqsubseteq c_1 \sqsubseteq \ldots \sqsubseteq c_n$ be a non-empty finite chain in S.

Then, $f(c_0) \sqsubseteq f(c_1) \sqsubseteq \ldots \sqsubseteq f(c_n)$ because f is monotone.

Thus, $f(\bigsqcup C) = f(c_n) = \bigsqcup f(C)$.



finite height



infinite height but all chains are finite

Fixpoints

Definition (Fixpoints)

Let $(S, \sqsubseteq)$ be a poset and $f : S \to S$ be a function. Then,

- a **fixpoint** of f is an element $x \in S$ such that $f(x) = x$
- a **pre-fixpoint** of f is an element $x \in S$ such that $f(x) \sqsubseteq x$
- a **post-fixpoint** of f is an element $x \in S$ such that $x \sqsubseteq f(x)$
- the **least fixpoint** of f is the minimum among fixpoints
- the **greatest fixpoint** of f is the maximum among fixpoints

We use the notations $\mathbf{lfp}(f)$ and $\mathbf{gfp}(f)$ to denote the least and greatest fixpoints of f, respectively, if they exist.

We use the notation $\mathbf{fix}(f)$ to denote the set of all fixpoints of f:

$$\mathbf{fix}(f) = \{x \in S \mid f(x) = x\}$$

Tarski's Fixpoint Theorem

Theorem (Tarski's Fixpoint Theorem)

Let $(S, \sqsubseteq)$ *be a complete lattice and* $f : S \to S$ *be a monotone function. Then, the following hold:*

- $\mathbf{lfp}(f) = \bigsqcap\{x \in S \mid f(x) \sqsubseteq x\}$ *is the least fixpoint of* f
- $\mathbf{gfp}(f) = \bigsqcup\{x \in S \mid x \sqsubseteq f(x)\}$ *is the greatest fixpoint of* f
- $\mathbf{fix}(f)$ *is a complete lattice*

Tarski's Fixpoint Theorem

Theorem (Tarski's Fixpoint Theorem)

Let $(S, \sqsubseteq)$ be a complete lattice and $f : S \to S$ be a monotone function. Then, the following hold:

- $\mathbf{lfp}(f) = \bigsqcap\{x \in S \mid f(x) \sqsubseteq x\}$ *is the least fixpoint of* f
- $\mathbf{gfp}(f) = \bigsqcup\{x \in S \mid x \sqsubseteq f(x)\}$ *is the greatest fixpoint of* f
- $\mathbf{fix}(f)$ *is a complete lattice*

However, it has two limitations:

- It is **not constructive**. It does not provide how to compute the least or greatest fixpoint.
- We **cannot apply** it to posets that are **not complete lattices**. For example, $(X \rightharpoonup Y, \sqsubseteq)$ is a CPO but not a complete lattice.

Kleene's Fixpoint Theorem

Theorem (Kleene's Fixpoint Theorem)

Let $(S, \sqsubseteq)$ be a CPO and $f : S \to S$ be a continuous function. Then,

$$\mathbf{lfp}(f) = \bigsqcup_{n \in \mathbb{N}} f^n(\bot)$$

Kleene's Fixpoint Theorem

PLRG

Theorem (Kleene's Fixpoint Theorem)

Let $(S, \sqsubseteq)$ be a CPO and $f : S \to S$ be a continuous function. Then,

$$\mathbf{lfp}(f) = \bigsqcup_{n \in \mathbb{N}} f^n(\bot)$$

- $\bigsqcup_{n \in \mathbb{N}} f^n(\bot)$ **exists in** S.

  Since f is continuous, it is monotone.

  Thus, $\{f^n(\bot) \mid n \in \mathbb{N}\}$ is a chain because:

  $$\bot \sqsubseteq f(\bot) \implies f(\bot) \sqsubseteq f^2(\bot) \implies f^2(\bot) \sqsubseteq f^3(\bot) \implies \ldots$$

  Since $(S, \sqsubseteq)$ is a CPO, $\bigsqcup_{n \in \mathbb{N}} f^n(\bot)$ exists in S.

Kleene's Fixpoint Theorem

- $\bigsqcup_{n \in \mathbb{N}} f^n(\bot)$ **is a fixpoint.**

$$\begin{array}{rcll} f(\bigsqcup_{n \in \mathbb{N}} f^n(\bot)) & = & \bigsqcup_{n \in \mathbb{N}} f(f^n(\bot)) & (\because f \text{ is continuous}) \\ & = & \bigsqcup_{n \in \mathbb{N}} f^{n+1}(\bot) & (\because f^{n+1} = f \circ f^n) \\ & = & \bot \sqcup \bigsqcup_{n \in \mathbb{N}} f^{n+1}(\bot) & (\because \bot \text{ is the minimum}) \\ & = & \bigsqcup_{n \in \mathbb{N}} f^n(\bot) & \end{array}$$

Kleene's Fixpoint Theorem

- $\bigsqcup_{n \in \mathbb{N}} f^n(\bot)$ **is a fixpoint**.

$$
\begin{array}{rcll}
f(\bigsqcup_{n \in \mathbb{N}} f^n(\bot)) & = & \bigsqcup_{n \in \mathbb{N}} f(f^n(\bot)) & (\because f \text{ is continuous}) \\
& = & \bigsqcup_{n \in \mathbb{N}} f^{n+1}(\bot) & (\because f^{n+1} = f \circ f^n) \\
& = & \bot \sqcup \bigsqcup_{n \in \mathbb{N}} f^{n+1}(\bot) & (\because \bot \text{ is the minimum}) \\
& = & \bigsqcup_{n \in \mathbb{N}} f^n(\bot) &
\end{array}
$$

- $\bigsqcup_{n \in \mathbb{N}} f^n(\bot)$ **is the least fixpoint**.

  Let $x \in S$ be a fixpoint of f. Then, $\bot \sqsubseteq x$ because $\bot$ is the minimum.

  Thus, $f(\bot) \sqsubseteq f(x) = x$ because f is monotone.

  By induction on n, we can show that $f^n(\bot) \sqsubseteq x$ for all $n \in \mathbb{N}$.

  Thus, x is an upper bound of $\{f^n(\bot) \mid n \in \mathbb{N}\}$, and hence $\bigsqcup_{n \in \mathbb{N}} f^n(\bot) \sqsubseteq x$.

`while` Statements in IMP

$$S[\![\texttt{while } e \texttt{ do } s]\!] \triangleq \mathbf{lfp}(F) = \bigcup_{n \in \mathbb{N}} F^n(\varnothing)$$

where

$$F(f)(\sigma) = \begin{cases} \sigma & \text{if } E[\![e]\!](\sigma) = \texttt{false} \\ f(S[\![s]\!](\sigma)) & \text{if } E[\![e]\!](\sigma) = \texttt{true} \\ \text{undefined} & \text{otherwise} \end{cases}$$

The poset $(\Sigma \rightharpoonup \Sigma, \sqsubseteq)$ is a CPO. We need to show that $F : (\Sigma \rightharpoonup \Sigma) \to (\Sigma \rightharpoonup \Sigma)$ is continuous to apply Kleene's fixpoint theorem.

Since function composition preserves continuity, it suffices to show that the following functions are continuous:

- $E[\![e]\!] : \Sigma \rightharpoonup \mathbb{V}$ and $S[\![s]\!] : \Sigma \rightharpoonup \Sigma$
- $\lambda f.\lambda\sigma. \begin{cases} \sigma & \text{if } \neg e(\sigma) \\ f(s(\sigma)) & \text{if } e(\sigma) \\ \text{undefined} & \text{otherwise} \end{cases}$ for some $e : \Sigma \rightharpoonup \mathbb{V}$ and $s : \Sigma \rightharpoonup \Sigma$

`while` Statements in NIMP

$$S[\![\texttt{while}\ e\ \texttt{do}\ s]\!] \triangleq \textbf{lfp}(F) = \bigcup_{n\in\mathbb{N}} F^n(\varnothing)$$

where

$$\begin{array}{rcl} F(g)(X) & \triangleq & g(S[\![s]\!](\{\sigma \in X \mid \texttt{true} \in E[\![e]\!](\sigma)\})) \cup \\ & & \{\sigma \in X \mid \texttt{false} \in E[\![e]\!](\sigma)\} \end{array}$$

To apply Kleene's fixpoint theorem, we need to show that $(\Sigma \to \mathcal{P}(\Sigma), \dot{\subseteq})$ is a CPO and $F : (\Sigma \to \mathcal{P}(\Sigma)) \to (\Sigma \to \mathcal{P}(\Sigma))$ is continuous.

Similar to IMP, it suffices to show that the following functions are continuous:

- $E[\![e]\!] : \Sigma \to \mathcal{P}(\mathbb{V})$ and $S[\![s]\!] : \Sigma \to \mathcal{P}(\Sigma)$
- $\lambda f.\lambda X.f(s(\{\sigma \in X \mid \texttt{true} \in e(\sigma)\})) \cup \{\sigma \in X \mid \texttt{false} \in e(\sigma)\}$ for some $e : \Sigma \to \mathcal{P}(\mathbb{V})$ and $s : \Sigma \to \mathcal{P}(\Sigma)$

Next Lecture

- Trace Semantics

Jihyeok Park
jihyeok_park@korea.ac.kr
https://plrg.korea.ac.kr