Probabilistic Programming

Lecture #5: Domain Theory

Joost-Pieter Katoen

Software Modeling and Verification Chair | RWTH AACHEN UNIVERSITY

RWTH Lecture Series on Probabilistic Programming 2018

Overview

Aims and sufficient conditions

- In denotational program semantics, the semantics of a loop is defined as some fixed point of a mathematical function
  - We will consider this for pGCL

$$f(x) = x$$

Aims and sufficient conditions

- In denotational program semantics, the semantics of a loop is defined as some fixed point of a mathematical function
  - We will consider this for pGCL

$$f(x) = x$$

- Goals:
  - Prove existence of such fixed points
  - Show how they can be "computed" (more exactly: approximated)

Aims and sufficient conditions

- In denotational program semantics, the semantics of a loop is defined as some fixed point of a mathematical function
  - We will consider this for pGCL
- Goals:
  - Prove existence of such fixed points
  - Show how they can be "computed" (more exactly: approximated)
- Sufficient conditions:

  $f : D \to D$

  - on function domains: complete lattices
  - on functions: monotonicity and Scott continuity

Overview

Partial orders

Partial order

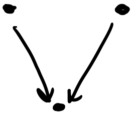
A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \subseteq D \times D$ such that, for every $d_1, d_2, d_3 \in D$:

- $d_1 \sqsubseteq d_1$ (reflexivity)
- $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \implies d_1 \sqsubseteq d_3$ (transitivity)
- $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \implies d_1 = d_2$ (antisymmetry)

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

$d_2 \sqsubseteq d_1$

$d_3 \sqsubseteq d_2$



Partial orders

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 $d_1, d_2, d_3 \in D$:

- $d_1 \sqsubseteq d_1$ (reflexivity)
- $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \implies d_1 \sqsubseteq d_3$ (transitivity)
- $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \implies d_1 = d_2$ (antisymmetry)

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

Examples

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

Partial orders

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 $d_1, d_2, d_3 \in D$:

- $d_1 \sqsubseteq d_1$ (reflexivity)
- $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \implies d_1 \sqsubseteq d_3$ (transitivity)
- $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \implies d_1 = d_2$ (antisymmetry)

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

Examples

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

Partial orders

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 $d_1, d_2, d_3 \in D$:

- $d_1 \sqsubseteq d_1$ (reflexivity)
- $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \implies d_1 \sqsubseteq d_3$ (transitivity)
- $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \implies d_1 = d_2$ (antisymmetry)

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

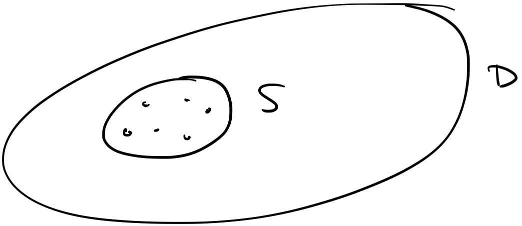
Examples

1. $(\mathbb{N}, \leqslant)$ 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)

Upper and lower bounds

Upper bound

An element $d \in D$ is called an upper bound of $S \subseteq D$, denoted $S \sqsubseteq d$, if $s \sqsubseteq d$ for every $s \in S$.

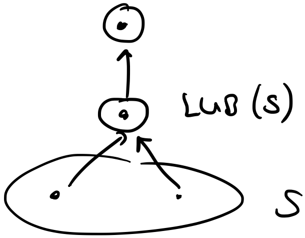


Upper and lower bounds

Upper bound

An element $d \in D$ is called an upper bound of $S \subseteq D$, denoted $S \sqsubseteq d$, if $s \sqsubseteq d$ for every $s \in S$.

An upper bound d of $S \subseteq D$ is called least upper bound (LUB) or supremum of S, denoted $d = \bigsqcup S$, if $d \sqsubseteq d'$ for every upper bound d' of S.



Upper and lower bounds

Upper bound

An element $d \in D$ is called an upper bound of $S \subseteq D$, denoted $S \sqsubseteq d$, if $s \sqsubseteq d$ for every $s \in S$.

An upper bound d of $S \subseteq D$ is called least upper bound (LUB) or supremum of S, denoted $d = \bigsqcup S$, if $d \sqsubseteq d'$ for every upper bound d' of S.

Lower bound

An element $d \in D$ is called a lower bound of $S \subseteq D$, denoted $d \sqsubseteq S$, if $d \sqsubseteq s$ for every $s \in S$.

Upper and lower bounds

$\langle 2^{\mathbb{N}}, \subseteq \rangle$ $S = \{\{1,2,3,4\}, \{2,4\}\}$

$glb(S) = \{2,4\}$

Upper bound

An element $d \in D$ is called an upper bound of $S \subseteq D$, denoted $S \sqsubseteq d$, if $s \sqsubseteq d$ for every $s \in S$.

An upper bound d of $S \subseteq D$ is called least upper bound (LUB) or supremum of S, denoted $d = \bigsqcup S$, if $d \sqsubseteq d'$ for every upper bound d' of S.

Lower bound

An element $d \in D$ is called a lower bound of $S \subseteq D$, denoted $d \sqsubseteq S$, if $d \sqsubseteq s$ for every $s \in S$.

A lower bound d of $S \subseteq D$ is called greatest lower bound (GLB) or infimum of S, denoted $d = \bigsqcap S$, if $d' \sqsubseteq d$ for every lower bound d' of S.

Chains

Chains

$S \subseteq D$ 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

Chains

$S \subseteq D$ 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.

A chain $S = s_1 \sqsubseteq s_2 \sqsubseteq s_3 \sqsubseteq \ldots$ is a ascending.
A chain $S = s_1 \sqsupseteq s_2 \sqsupseteq s_3 \sqsupseteq \ldots$ is a descending.

Examples: chains

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

Examples: chains

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

Complete lattices

Complete lattice

A PO $(D, \sqsubseteq)$ is called a complete lattice, if every subset $S \subseteq D$ has a supremum in D, i.e., $\bigsqcup S \in D$.

Complete lattices

Complete lattice

A PO $(D, \sqsubseteq)$ is called a complete lattice, if every subset $S \subseteq D$ has a supremum in D, i.e., $\bigsqcup S \in D$.

Every complete lattice $(D, \sqsubseteq)$ has a least element $\bot$ and, dually, a greatest element $\top$ which satisfy:

$$\forall d \in D. \quad \bot \sqsubseteq d \sqsubseteq \top \ .$$

by definition $\emptyset \subseteq D$

by definition every $d \in D$ is an upper bound of $\emptyset$

thus $\bigsqcup \emptyset$ exists and is the least elt $\bot$ of $(D, \sqsubseteq)$

Complete lattices

Complete lattice

A PO $(D, \sqsubseteq)$ is called a complete lattice, if every subset $S \subseteq D$ has a supremum in D, i.e., $\bigsqcup S \in D$.

Every complete lattice $(D, \sqsubseteq)$ has a least element $\perp$ and, dually, a greatest element $\top$ which satisfy:

$$\forall d \in D. \quad \perp \sqsubseteq d \sqsubseteq \top \ .$$

For complete lattice $(D, \sqsubseteq)$: every subset $S \subseteq D$ has an infimum in D, i.e., $\bigsqcap S \in D$.

Every ascending or descending chain has a least upper bound and greatest lower bound.

Every $S \subseteq D$ has a glb ($=$ inf) $\bigsqcup S \in D$.

Proof let $(D, \sqsubseteq)$ be a complete lattice and let $S \subseteq D$. let L be the set of all lower bounds of S i.e.

$$L = \{ d \in D \mid \forall s \in S .\ d \sqsubseteq s \}$$

As $L \subseteq D$, and $(D, \sqsubseteq)$ is a compl. lattice

$\sup L \in D$

But then $\sup L$ is the largest lower bounds of S i.e. $\sup L = \inf S$ $\boxtimes$

Examples: lattices

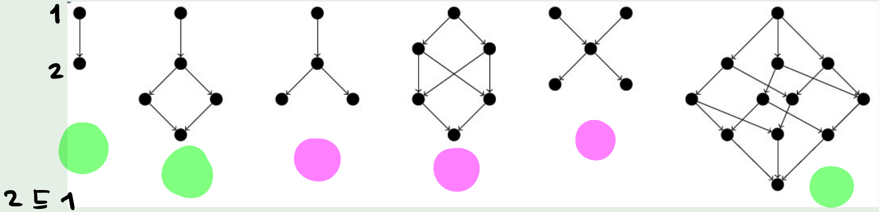
1. $(2^{\mathbb{N}}, \subseteq)$ is a complete lattice with $\bigsqcup S = \bigcup_{M \in S} M$ for every subset $S \subseteq 2^{\mathbb{N}}$.

Examples: lattices

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

Examples: lattices

1. $(2^{\mathbb{N}}, \subseteq)$ is a complete lattice with $\bigsqcup S = \bigcup_{M \in S} M$ for every subset $S \subseteq 2^{\mathbb{N}}$.
2. $(\mathbb{N}, \leqslant)$ is not a complete lattice, as, e.g., the chain $\mathbb{N}$ has no upper bound.
3. Which of the following structures are complete lattices?



Note: a lattice* with a top $\top$ and a bottom element $\bot$ is <u>not</u> necessarily a complete lattice. Example (due to Lifschitz):

let $R = \mathbb{Q} \cap [0,1]$. Then: $(R, \leq)$ is a lattice with a $\bot = 0$ and $\top = 1$.

let x be an irrational number in $[0,1]$, and $I_x = \{r \in R \mid r \leq x\} \subseteq R$.

Then: I_x has no supremum in R.

* PO $(D, \sqsubseteq)$ is a lattice if each two-element subset $S \subseteq D$ has a supremum (and infimum).

Overview

Monotonicity

Monotonicity

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be partial orders, and let $F : D \to D'$. F is called monotonic (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every $d_1, d_2 \in D$,

$$d_1 \sqsubseteq d_2 \quad \text{implies} \quad F(d_1) \sqsubseteq' F(d_2).$$

Monotonicity

Monotonicity

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be partial orders, and let $F : D \to D'$. F is called monotonic (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every $d_1, d_2 \in D$,

$$d_1 \sqsubseteq d_2 \quad \text{implies} \quad F(d_1) \sqsubseteq' F(d_2).$$

Interpretation: monotonic functions preserve information

Monotonicity

Monotonicity

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be partial orders, and let $F : D \to D'$. F is called monotonic (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every $d_1, d_2 \in D$,

$$d_1 \sqsubseteq d_2 \quad \text{implies} \quad F(d_1) \sqsubseteq' F(d_2).$$

Interpretation: monotonic functions preserve information

1. Let $T := \{S \subseteq \mathbb{N} \mid S \text{ finite}\}$. Then $F_1 : T \to \mathbb{N} : S \mapsto \sum_{n \in S} n$ is monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$ and $(\mathbb{N}, \leqslant)$.

$T = \{2, 27, 301\}$

$F_1 = 2 + 27 + 301$

Monotonicity

Monotonicity

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be partial orders, and let $F : D \to D'$. F is called monotonic (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every $d_1, d_2 \in D$,

$$d_1 \ \sqsubseteq \ d_2 \quad \text{implies} \quad F(d_1) \ \sqsubseteq' \ F(d_2).$$

Interpretation: monotonic functions preserve information

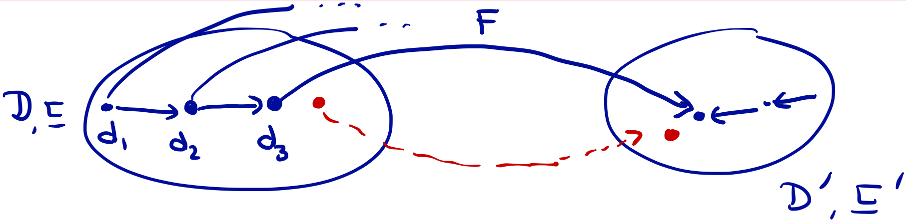
1. Let $T := \{S \subseteq \mathbb{N} \mid S \text{ finite}\}$. Then $F_1 : T \to \mathbb{N} : S \mapsto \sum_{n \in S} n$ is monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$ and $(\mathbb{N}, \leqslant)$.
2. $F_2 : 2^{\mathbb{N}} \to 2^{\mathbb{N}} : S \mapsto \mathbb{N} \setminus S$ is not monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$ (since, e.g., $\varnothing \subseteq \mathbb{N}$ but $F_2(\varnothing) = \mathbb{N} \nsubseteq F_2(\mathbb{N}) = \varnothing$).

Monotonicity on chains

The following lemma states how chains behave under monotonic functions.

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be complete lattices, $F : D \to D'$ monotonic, and $S \subseteq D$ a chain in D. Then:

1. $F(S) := \{ F(d) \mid d \in S \}$ is a chain in D'.
2. $\bigsqcup F(S) \sqsubseteq' F(\bigsqcup S)$.



Monotonicity on chains

The following lemma states how chains behave under monotonic functions.

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be complete lattices, $F : D \to D'$ monotonic, and $S \subseteq D$ a chain in D. Then:

1. $F(S) := \{ F(d) \mid d \in S \}$ is a chain in D'.
2. $\bigsqcup F(S) \sqsubseteq' F(\bigsqcup S)$.

Proof.

Left as a homework exercise. $\square$

Scott continuity

A function F is continuous if applying F and taking LUBs is commutable:

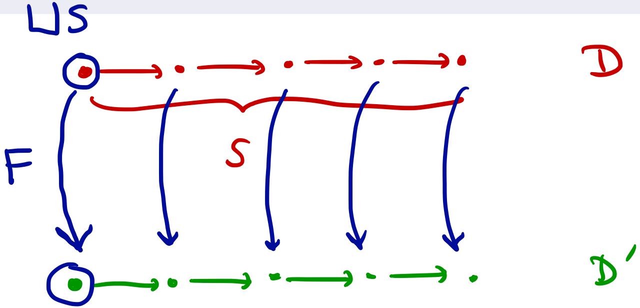
Scott continuity

A function F is continuous if applying F and taking LUBs is commutable:

Scott continuity

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be complete lattices and $F : D \to D'$ monotonic. Then F is called continuous if, for every non-empty chain $S \subseteq D$,

$$F\left(\bigsqcup S\right) = \bigsqcup F(S).$$



Scott continuity

A function F is continuous if applying F and taking LUBs is commutable:

Scott continuity

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be complete lattices and $F : D \to D'$ monotonic. Then F is called continuous if, for every non-empty chain $S \subseteq D$,

$$F\left(\bigsqcup S\right) = \bigsqcup F(S).$$

Every continuous function is monotonic.

Scott continuity

A function F is continuous if applying F and taking LUBs is commutable:

Scott continuity

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be complete lattices and $F : D \rightarrow D'$ monotonic. Then F is called continuous if, for every non-empty chain $S \subseteq D$,

$$F\left(\bigsqcup S\right) = \bigsqcup F(S).$$

Every continuous function is monotonic.

Proof.

1. Let $d \sqsubseteq e$. Then $\{ d, e \}$ is a chain with $\bigsqcup \{ d, e \} = e$.
2. Let F be continuous. Then $F(d) \sqsubseteq \bigsqcup \{ F(d), F(e) \}$.
3. By continuity of F, $\{ F(d), F(e) \} = F(\bigsqcup \{ d, e \})$, which equals $F(d)$.

Overview

1. Motivation
2. Complete lattices
3. Monotonic and continuous functions
4. Fixpoint theorems

$$f(x) = x$$

$$\Leftrightarrow$$

$$f(x) - x = 0$$

Fixed points

Fixed point

Let $F : D \to D$ be a function. Element $d \in D$ is called a fixed point of F if and only if $F(d) = d$.

Fixed points

Fixed point

Let $F : D \to D$ be a function. Element $d \in D$ is called a fixed point of F if and only if $F(d) = d$.

Examples

1. Function $F : \mathbb{R} \to \mathbb{R}$ with $F(x) = x^2 - 3x + 4$ has a fixed point at 2.
2. For function $F : \mathbb{R} \to \mathbb{R}$ with $F(x) = x$, all $x \in \mathbb{R}$ are fixed points.
3. Function $F : \mathbb{R} \to \mathbb{R}$ with $F(x) = x+4$ has no fixed points.
4. Function $F : \mathbb{R} \to \mathbb{R}$ with $F(x) = \frac{x}{2} + \frac{1}{x}$ has a fixed point at $\sqrt{2}$.
5. Function $F : \mathbb{R} \to \mathbb{R}$ with $F(x) = \cos(x)$ has a fixed point, but this is hard to determine.

How to find fixed points?

Naive scheme: start with an initial value x_0, and then iterate: $x_{n+1} = f(x_n)$.

How to find fixed points?

Naive scheme: start with an initial value x_0, and then iterate: $x_{n+1} = f(x_n)$.

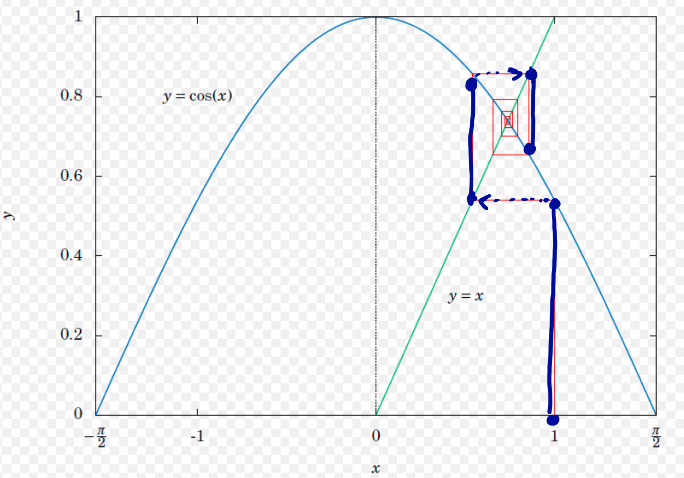
(Wrong) idea: as n grows larger, x_n converges to some fixed point of F.

1. Take $F(x) = \frac{x}{2} + \frac{1}{x}$ and $x_0 = 1$. Iterations yields: $\frac{3}{2}, \frac{17}{12}, \frac{17}{24} + \frac{12}{17}$ which indeed approximates $\sqrt{2}$.
2. Take $F(x) = \frac{5}{2}x - \frac{3}{2}x^2$. Iteration converges to 1.
3. But, take $F(x) = \frac{13}{4}x - \frac{3}{2}x^2$. Iteration oscillates between two points, regardless of the initial value.

When does such an iterative scheme (i.e., approximate) a fixed point, and if so, which fixed point?

We consider this for complete lattices and continuous functions.

Iterative scheme to determine a fixed point



cos(1), cos(cos(1)), cos(cos(cos(1))). . etc.

Kleene's fixpoint theorem

Kleene's fixpoint theorem

Let $(D, \sqsubseteq)$ be a complete lattice and $F : D \to D$ continuous. Then F has a least fixed point $\text{lfp}\, F$ and greatest fixed point $\text{gfp}\, F$ respectively, given by:

$$\text{lfp}\, F := \sup_{n \in \mathbb{N}} F^n(\bot) \quad \text{and} \quad \text{gfp}\, F := \inf_{n \in \mathbb{N}} F^n(\top)$$

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

Lfp F: = lub of the set

$$\{\underbrace{F^0(\bot)}_{=\bot}, F(\bot), F^2(\bot), F^3(\bot), \ldots, F^{1001}(\bot), \ldots\}$$

Proof

Let $X = \bigsqcup_n F^n(\bot)$

(a) Claim: X is a fixed point of F.

$$
\begin{aligned}
F(X) &= F\left(\bigsqcup_n F^n(\bot)\right) && \text{by def. } X \\
&= \bigsqcup_n F(F^n(\bot)) && \text{by continuity of } F \\
&= \bigsqcup_n F^{n+1}(\bot) \\
&= \bot \sqcup \bigsqcup_n F^{n+1}(\bot) && \text{as } \bot \text{ is the least element} \\
&= F^0(\bot) \sqcup \bigsqcup_n F^{n+1}(\bot) \\
&= \bigsqcup_n F^n(\bot) \\
&= X
\end{aligned}
$$

claim:

(b) $X = \bigsqcup_n F^n(\bot)$ is the least fixed point

Let $Y \neq X$ be a fixed point of F.

It follows (by induction on n)

that $\boxed{F^n(\bot) \sqsubseteq Y \quad \forall n.}$

Since every element of the chain

$$F^0(\bot) \sqsubseteq F^1(\bot) \sqsubseteq F^2(\bot) \sqsubseteq \dots$$

is a subset of Y we have

$$X = \bigsqcup_n F^n(\bot) \sqsubseteq Y$$

so X is the least fixed point $\boxtimes$

Kleene's fixpoint theorem

Kleene's fixpoint theorem

Let $(D, \sqsubseteq)$ be a complete lattice and $F : D \to D$ continuous. Then F has a least fixed point $\mathrm{lfp}\, F$ and greatest fixed point $\mathrm{gfp}\, F$ respectively, given by:

$$\mathrm{lfp}\, F := \sup_{n \in \mathbb{N}} F^n(\bot) \quad \text{and} \quad \mathrm{gfp}\, F := \inf_{n \in \mathbb{N}} F^n(\top)$$

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

Proof.

on the board □

Examples

- Domain: complete lattice $(2^{\mathbb{N}}, \subseteq)$ with $\bigsqcup S = \bigcup_{N \in S} N$

Examples

- Domain: complete lattice $(2^{\mathbb{N}}, \subseteq)$ with $\bigsqcup S = \bigcup_{N \in S} N$
- Function: $F : 2^{\mathbb{N}} \to 2^{\mathbb{N}} : N \mapsto N \cup A$ for some fixed $A \subseteq \mathbb{N}$
  - F monotonic: $M \subseteq N \implies F(M) = M \cup A \subseteq N \cup A = F(N)$
  - F continuous: $F(\bigsqcup S) = F\left(\bigcup_{N \in S} N\right) = \left(\bigcup_{N \in S} N\right) \cup A = \bigcup_{N \in S} (N \cup A) = \bigcup_{N \in S} F(N) = \bigsqcup F(S)$.

Examples

- Domain: complete lattice $(2^{\mathbb{N}}, \subseteq)$ with $\bigsqcup S = \bigcup_{N \in S} N$
- Function: $F : 2^{\mathbb{N}} \to 2^{\mathbb{N}} : N \mapsto N \cup A$ for some fixed $A \subseteq \mathbb{N}$
  - F monotonic: $M \subseteq N \implies F(M) = M \cup A \subseteq N \cup A = F(N)$
  - F continuous: $F(\bigsqcup S) = F\left(\bigcup_{N \in S} N\right) = \left(\bigcup_{N \in S} N\right) \cup A = \bigcup_{N \in S} (N \cup A) = \bigcup_{N \in S} F(N) = \bigsqcup F(S)$.
- Fixpoint iteration: $N_n := F^n(\bigsqcup \varnothing)$ where $\bigsqcup \varnothing = \varnothing$ $\quad \bot = \varnothing$
  - $N_0 = \bigsqcup \varnothing = \varnothing$
  - $N_1 = F(N_0) = \varnothing \cup A = A$
  - $N_2 = F(N_1) = A \cup A = A = N_n$ for every $n \geq 1$

$\Rightarrow$ gfp $F = A$

Examples

- Domain: complete lattice $(2^{\mathbb{N}}, \subseteq)$ with $\bigsqcup S = \bigcup_{N \in S} N$
- Function: $F : 2^{\mathbb{N}} \to 2^{\mathbb{N}} : N \mapsto N \cup A$ for some fixed $A \subseteq \mathbb{N}$
  - F monotonic: $M \subseteq N \implies F(M) = M \cup A \subseteq N \cup A = F(N)$
  - F continuous: $F(\bigsqcup S) = F\left(\bigcup_{N \in S} N\right) = \left(\bigcup_{N \in S} N\right) \cup A = \bigcup_{N \in S}(N \cup A) = \bigcup_{N \in S} F(N) = \bigsqcup F(S)$.
- Fixpoint iteration: $N_n := F^n(\bigsqcup \varnothing)$ where $\bigsqcup \varnothing = \varnothing$
  - $N_0 = \bigsqcup \varnothing = \varnothing$
  - $N_1 = F(N_0) = \varnothing \cup A = A$
  - $N_2 = F(N_1) = A \cup A = A = N_n$ for every $n \geq 1$

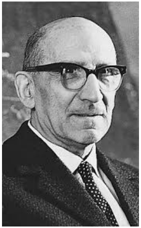
  $\Rightarrow$ gfp $F = A$
- Alternatively: $F(N) = N \cap A$

  $\Rightarrow$ gfp $F = \varnothing$

Knaster-Tarski theorem (1)

Alfred Tarski (1901–1983)

Bronislaw Knaster (1893–1990)



Prefixed point and postfixed point

For monotonic function $F : D \rightarrow D$ on $(D, \sqsubseteq)$ and $d \in D$:

1. d is a prefixed point of F if $F(d) \sqsubseteq d$
2. d is a postfixed point of F if $d \sqsubseteq F(d)$.

d is a prefixed and a postfixed point of F iff d is a fixed point.

Knaster-Tarski theorem (2)

F is monotonic

Knaster-Tarski theorem

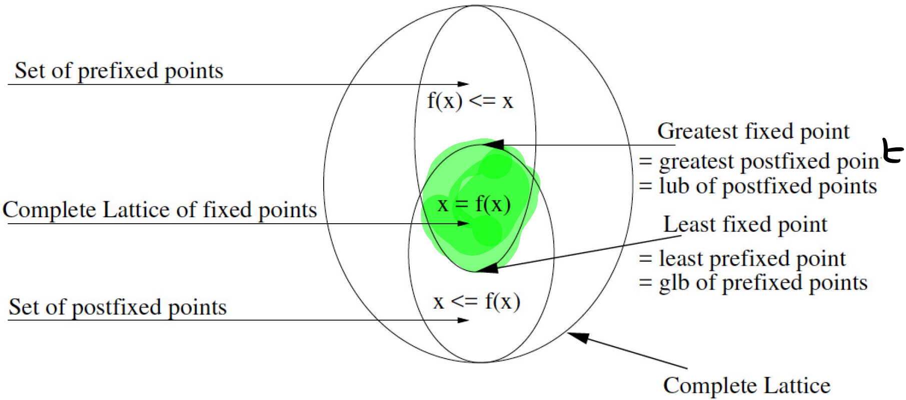
For any complete lattice $(D, \sqsubseteq)$ the following holds:

1. The least fixed and the least prefixed points of F exist, and are identical
2. The greatest fixed and the greatest postfixed points of F exist, and are identical
3. The fixed points of F form a complete lattice. !!

Proof.

On the black board. □

Pictorial depiction of the Knaster-Tarski theorem



$(D, \sqsubseteq)$ is a complete lattice

Proof

$F: D \to D$ monotonic

(1) let pre be the set of prefixed points of F

let p be the glb = inf pre.

p does exist as we deal with complete lattices. <u>Claim</u>: p is the least prefixed point of F, and p is the lfp F.

let $x \in$ pre.

a. $p \sqsubseteq x$ (* as p = inf pre *)

$\Rightarrow F(p) \sqsubseteq F(x)$ (* as F is monotonic *)

$\Rightarrow F(p) \sqsubseteq x$ (* as $x \in$ pre *)

$\Rightarrow$ (* as $x \in$ pre is arbitrary, it follows that F(p) is a Lb of pre; now as p = glb pre *)

$F(p) \sqsubseteq p$

$\Rightarrow$ (* thus by definition $p \in$ pre; in addition p is a Lb of pre *)

p is the least prefixed point of F

b. p is the Lfp F:

$F(p) \sqsubseteq p$ (* since p is a prefixed point)

$\Rightarrow F(F(p)) \sqsubseteq F(p)$ (* by monotonicity *)

$\Rightarrow$ (* $F(p)$ is a prefixed point by def. + p is a lb ~~pre~~ *)

$p \sqsubseteq F(p)$

$\Rightarrow$ (* p is a prefixed point so $F(p) \sqsubseteq p$ *)

$p = F(p)$

$\Rightarrow$ p is a fixed point of F

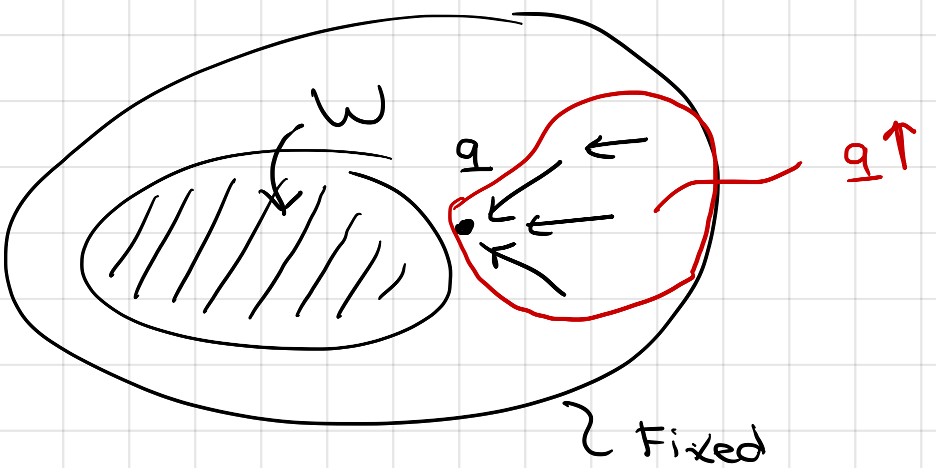
$\wedge$ p is lowerbound over prefixed points

$\Rightarrow$ p is lb over all fixed points

$\Rightarrow$ p is a least fixed point

(3) The fixed points of F form a complete lattice.

Let W be a subset of fixed points of F



$\boxed{\text{Show: existence of } \sup W.}$

Let $q = \bigsqcup W$. Let $q\uparrow = \{ w \mid q \sqsubseteq w \}$

Then $q \in q\uparrow$, and by def. of $q\uparrow$, $q = \inf q\uparrow$

(a) $q\uparrow$ is a complete lattice

(b) F maps $q\uparrow$ onto $q\uparrow$ (* monotonicity *)

(c) F is a mapping over $\underbrace{(q\uparrow, \sqsubseteq)}_{\text{complete lattice}}$

$\Rightarrow$ q is glb of $q\uparrow$

proofs of (a) through (c)

(a) claim: $q\uparrow$ is a complete lattice. Proof:

as $q\uparrow \subseteq W$ and W is a complete lattice,

$\inf q\uparrow$ and $\sup q\uparrow$ exist and lie in W

We have $q = \inf q\uparrow$ and $q \in q\uparrow$, thus

$\inf q\uparrow \in q$. Furthermore, since $q \in q\uparrow$,

$q \sqsubseteq \sup q\uparrow$. By definition of $q\uparrow$, we

have $\sup q\uparrow \in q\uparrow$.

(b) claim: F maps $q\uparrow$ to $q\uparrow$. Let $w \in W$

and $x \in q\uparrow$. To show: $F(x) \in q\uparrow$.

We have: $w \sqsubseteq q$ and $q \sqsubseteq x$

$\Rightarrow$ (* monotonicity of F; transitivity of $\sqsubseteq$ *)

$F(w) \sqsubseteq F(x)$

$\Rightarrow$ (* W is a set of fixed points of F *)

$w \sqsubseteq F(x)$

$\Rightarrow$ (* w is an arbitrary elt of W *)

$\sup W \sqsubseteq F(x)$

(* $q = \sup W$ *)

$\Rightarrow$ $q \sqsubseteq F(x)$ $\Rightarrow$ $F(x) \in q\uparrow$.

(c) From (a) and (b), it follows that F is a mapping over the complete lattice $\underline{q}\uparrow$. Also: F is monotonic. Thus F has an lfp $\underline{q}'$ in $\underline{q}\uparrow$. Since $\underline{q} \sqsubseteq \underline{q}\uparrow$, $\underline{q} \sqsubseteq \underline{q}'$.

Thus: $\underline{q}' = \sup W$.