CS615: Formal Specification and Verification of Programs 2019

Lecture 11: Fixed points

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2019-09-17

Topic 11.1

Fixed point theory

Fixed points

Let X be a set.
A fixed point of a function $f : X \to X$ is $x \in X$ such that $f(x) = x$

Let f be a function on poset $(X, \leq)$:

- $fp(f) \triangleq \{x | f(x) = x\}$
- $prefp(f) \triangleq \{x | x \leq f(x)\}$
- $postfp(f) \triangleq \{x | f(x) \leq x\}$
- least fixed point $lfp(f) \triangleq min(fp(f))$
- greatest fixed point $gfp(f) \triangleq max(fp(f))$

lfp and gfp may not exist.

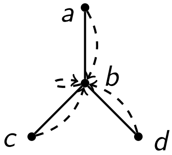
Exercise 11.1

$fp(f) = prefp(f) \cap postfp(f)$

Example: fixed points

Example 11.1

Consider the following poset and a function f (dashed-lines)



- $prefp(f) = \{c, d, b\}$
- $postfp(f) = \{a, b\}$
- $postfp(f) = \{b\}$

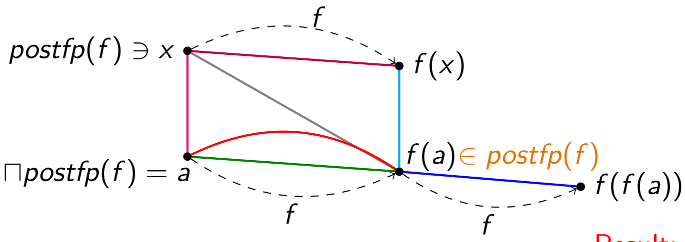
Knaster-Tarski fixed point theorem

Theorem 11.1

A monotonic map $f : X \to X$ on a complete lattice $(X, \sqsubseteq, \top, \bot, \sqcap, \sqcup)$ has a least fixed point, which is

$$lfp(f) = \sqcap postfp(f) = \sqcap\{x | f(x) \sqsubseteq x\}$$

Proof.



Reasons:
complete lattice $\Rightarrow \sqcap$ exist
$x \in postfp(f)$
f is monotone
transitivity
$f(a)$ is lb and a is glb
f is monotone
def. $postfp(f)$
def. $\sqcap postfp(f)$

Result: $f(a) = a \in postfp(f)$

Since $fp(f) \subseteq postfp(f)$, a is lfp. (why $postfp(f) \neq \emptyset$?) $\square$

Knaster-Tarski theorem for gfp

Theorem 11.2

A monotonic map $f : X \to X$ *on a complete lattice* $(X, \sqsubseteq, \top, \bot, \sqcap, \sqcup)$ *has a greatest fixed point, which is*

$$gfp(f) = \sqcup prefp(f) = \sqcup\{x | x \sqsubseteq f(x)\}$$

The proof is symmetrical to the previous case.

lfp greater than a prefix point

Definition 11.1

Let $f : X \to X$ be a monotonic map on a complete lattice $(X, \sqsubseteq, \top, \bot, \sqcap, \sqcup)$. Let $a \in X$. Let $lfp_a(f)$ be the least fixed point of f greater than a, i.e.,

$$a \sqsubseteq lfp_a(f) \qquad lfp_a(f) = f(lfp_a(f)) \qquad \forall x.\ a \sqsubseteq x = f(x) \Rightarrow lfp_a(f) \sqsubseteq x$$

Theorem 11.3

If $a \in prefp(f)$ then $lfp_a(f)$ exists and $lfp_a(f) = lfp(\lambda x.a \sqcup f(x))$.

Proof.

1. Let $p = lfp(\lambda x.a \sqcup f(x))$. So, $p = a \sqcup f(p)$.
2. By def. of $\sqcup$, $a \sqsubseteq p$, the first condition satisfied
3. Due to monotonic f, $f(a) \sqsubseteq f(p)$
4. Due to $a \sqsubseteq f(a)$ and transitivity, $a \sqsubseteq f(p)$
5. Therefore, $f(p) = a \sqcup f(p)$ and $p = f(p)$, the second condition satisfied
6. Choose q such that $a \sqsubseteq q$ and $q = f(q)$, then $a \sqcap f(q) = q$.
7. Therefore, $q \in postfp(\lambda x.a \sqcup f(x))$.
8. Kanaster-Tarski, $p \sqsubseteq q$, the third condition satisfied $\square$

Exercise: $lfp_a(f)$ may not exists

Exercise 11.2

Show if $a \notin prefp(f)$ then $lfp_a(f)$ may not exists.

Fixed point lattice

Theorem 11.4

Let $f : X \to X$ be a monotonic map on a complete lattice $(X, \sqsubseteq, \top, \bot, \sqcap, \sqcup)$. $fp(f)$ forms a complete lattice.

Exercise 11.3

For $S \subseteq fp(f)$, show that $lfp_{\sqcup S}(f)$ exists and is lub of X in poset $(fp(f), \sqsubseteq)$
Hint: use theorem 11.3

Fixed point compose

Theorem 11.5

Let $(X, \leq)$ and $(Y, \sqsubseteq)$ be complete lattices, and $f : X \to Y$ and $g : Y \to X$ are monotonic then

$$g(lfp(f \circ g)) = lfp(g \circ f)$$

Proof.

1. $(g \circ f)g((lfp(f \circ g))) = g(f \circ g(lfp(f \circ g))) = g(lfp(f \circ g))$
2. Therefore, $g(lfp(f \circ g))$ is a fixed point of $g \circ f$
3. Assume $x = g \circ f(x)$
4. $\Rightarrow f(x) = f \circ g \circ f(x) \Rightarrow f(x) = f \circ g(f(x))$
5. Therefore, by Kanaster-tarski, $lfp(f \circ g) \sqsubseteq f(x)$
6. Since g is monotone, $g(lfp(f \circ g)) \leq g \circ f(x)$
7. Due to 3, $g(lfp(f \circ g)) \leq x$
8. Therefore, $g(lfp(f \circ g))$ is lfp of $g \circ f$

□

Greater function

Theorem 11.6

Let $f, g : X \to X$ be monotonic maps on a complete lattice $(X, \sqsubseteq, \top, \bot, \sqcap, \sqcup)$ such that for all $x \in X$, $f(x) \sqsubseteq g(x)$ then

$$lfp(f) \sqsubseteq lfp(g)$$

Exercise 11.4

Prove the above theorem

Transfinite iterates

Let $f : X \rightarrow X$ be a function on a poset $(X, \sqsubseteq, \sqcap, \sqcup)$.

Definition 11.2

For some ordinal number λ, the upward iterates $(\mathrm{I}^k, k \leq \lambda)$ of f from a is a sequence such that

- $\mathrm{I}^0 = a$
- $\mathrm{I}^{k+1} = f(\mathrm{I}^k)$
- $\mathrm{I}^\lambda = \sqcup_{k<\lambda} \mathrm{I}^k$

Definition 11.3

For some ordinal number λ, the downward iterates $(\mathrm{I}^k, k \leq \lambda)$ of f from a is a sequence such that

- $\mathrm{I}^0 = a$
- $\mathrm{I}^{k+1} = f(\mathrm{I}^k)$
- $\mathrm{I}^\lambda = \sqcap_{k<\lambda} \mathrm{I}^k$

In poset, $\sqcap$ and $\sqcup$ are partially defined. Consequently, iterates are partially defined. If X is a lattice or cpo then iterates are well-defined.

Recall: Complete partial order

Definition 11.4

A complete partial order(cpo) is a poset $(X, \sqsubseteq)$ *such that every increasing chain in* X *has a lub in* X

A condition for finite iterates converging to lfp

Theorem 11.7

If

- $(X, \sqsubseteq, \sqcup, \sqcap)$ *is poset,*
- $f : X \to X$ *is a monotone function,*
- $a \in prefp(f)$,
- *upward iterates* $(\mathrm{I}^k, k \leq \omega)$ *of* f *from* a *exists, and*
- $\mathrm{I}^\omega \in fp(f)$

then $(\mathrm{I}^k, k \leq \omega)$ *is increasing chain and* $\mathrm{I}^\omega = lfp_a(f)$.

Assumed $\mathrm{I}^\omega \in fp(f)$.
When $\mathrm{I}^\omega \in fp(f)$?

Proof.

1. Since $a \sqsubseteq f(a)$, $\mathrm{I}^0 \sqsubseteq \mathrm{I}^1$
2. Induction hyp, $\mathrm{I}^n \sqsubseteq \mathrm{I}^{n+1}$. Due to monotone f, $f(\mathrm{I}^n) \sqsubseteq f(\mathrm{I}^{n+1}) \Rightarrow \mathrm{I}^{n+1} \sqsubseteq \mathrm{I}^{n+2}$
3. By induction, $\forall n < \omega.\ \mathrm{I}^n \sqsubseteq \mathrm{I}^{n+1}$
4. Since $\mathrm{I}^\omega = \sqcup_{k<\omega} \mathrm{I}^k$ and I^ω exists, $\forall n \leq m \leq \omega.\ \mathrm{I}^n \sqsubseteq \mathrm{I}^m$ (proved increasing chain)
5. Since $a = \mathrm{I}^0$, $a \sqsubseteq \mathrm{I}^\omega$
6. Assume $a = \mathrm{I}^0 \sqsubseteq x = f(x)$.Since f is monotone, $I^n \sqsubseteq x \Rightarrow \mathrm{I}^{n+1} = f(\mathrm{I}^n) \sqsubseteq f(x) = x$
7. By induction and def. of I^ω, $\forall n \leq \omega.\mathrm{I}^n \sqsubseteq x$.Therefore $\mathrm{I}^\omega = lfp_a(f)$

Kleene fixed point theorem

Theorem 11.8

If

- $(X, \sqsubseteq, \sqcup)$ *is cpo,*
- $f : X \to X$ *is upper continuous,*
- $a \in prefp(f)$*, and*
- $(\mathrm{I}^k, k \leq \omega)$ *be upward iterates of* f *from* a

then $\mathrm{I}^\omega = lfp_a(f)$*.*

Proof.

1. f is continuous $\Rightarrow$ f is monotone $\Rightarrow$ $(\mathrm{I}^k, k \leq \omega)$ increasing chain
2. Since X is cpo, I^ω exists.
3. $f(\mathrm{I}^\omega) = f(\sqcup_{k<\omega}\mathrm{I}^k)$
4. $= \sqcup_{k<\omega} f(\mathrm{I}^k)$, since f is continuous.
5. $= \sqcup_{0<k<\omega}\mathrm{I}^k = a \sqcup_{0<k<\omega} \mathrm{I}^k = \sqcup_{k<\omega}\mathrm{I}^k = \mathrm{I}^\omega$
6. Due to the previous theorem, $\mathrm{I}^\omega = lfp_a(f)$

Knaster-Tarski for CPOs

We can prove Knaster-Tarski Theorem like results on cpos.

Theorem 11.9

If

- $(X, \sqsubseteq, \sqcup)$ *is cpo,*
- $f : X \rightarrow X$ *is upper continuous, and*
- $a \in prefp(f)$

then $lfp_a(f) = \sqcap\{x \in X | a \sqsubseteq x \wedge f(x) \sqsubseteq x\}$.

Proof.

Let $P = \{x \in X | a \sqsubseteq x \wedge f(x) \sqsubseteq x\}$. Let $(\mathrm{I}^k, k \leq \omega)$ are iterates of f from a.

1. Due to previous theorem, $lfp_a(f) = \mathrm{I}^\omega$. And, $\mathrm{I}^\omega \in P$.
2. Choose x, $a \sqsubseteq x \in P$
3. Induction hyp, $\mathrm{I}^n \leq x \Rightarrow f(\mathrm{I}^n) \leq f(x) \leq x \Rightarrow \mathrm{I}^{n+1} \leq x$
4. By induction, $\forall n < \omega, \mathrm{I}^n \leq x$.
5. By def. of I^ω, $\mathrm{I}^\omega \leq x$
6. Therefore, $lfp_a(f) \sqsubseteq \sqcap P$

Fixed point for monotone functions on cpos

Theorem 11.10

If

- $(X, \sqsubseteq, \sqcup)$ *is cpo,*
- $f : X \to X$ *is monotone function,*
- $a \in prefp(f)$*, and*
- *for some ordinal* λ, $(\mathrm{I}^k, k \leq \lambda)$ *be upward iterates of* f *from* a

then $(\mathrm{I}^k, k \leq \lambda)$ *is increasing chain, which is ultimately stationary and converges to* $lfp_a(f)$*.*

Monotone is a weaker condition than continuous. Therefore, we need larger ordinals

We will skip the proof. However, the length to the stationary point is bounded by the ordinal size of the cpo

Topic 11.2

Asynchronous iterations for fixed points

System of simultaneous fixed point equations

For $i \in 1..n$, $(X_i, \sqsubseteq_i, \bot_i, \top_i, \sqcup_i, \sqcap_i)$ be complete lattices.

Let complete lattice $(X, \sqsubseteq, \bot, \top, \sqcup, \sqcap)$ be

- $X = X_1 \times \cdots \times X_n$
- $x \sqsubseteq y = (\wedge_{i=1}^{n} x_i \sqsubseteq_i y_i)$

Let $f : X \times X$ and $f_i : X \times X_i$ be $f_i(X) = (f(X))_i$

The fixed point equation $x = f(x)$ can be written as the following simultaneous fixed point equation.

$$
\begin{aligned}
x_1 =& f_1(x_1, \dots, x_n) \\
&\vdots \\
x_n =& f_n(x_1, \dots, x_n)
\end{aligned}
$$

Asynchronous iterations

We need not update each component at each iteration. We only need to ensure that each component is updated fairly.

Definition 11.5 (Chaotic iterations)

Let $(J^k, k \in \mathbb{O})$ *be a sequence of subsets of* $[1, n]$, *which is weakly fair, i.e.,*

$$\forall i \in 1..n\ \forall j \in \mathbb{O}.\ \exists k > j.\ i \in J^k$$

The *iterates* $(\mathrm{I}^k, k < \lambda)$ *starting from* $a \in X$ *for* F *defined by* $(J^k, k \in \mathbb{O})$ *is*

$$\begin{aligned}
&\mathrm{I}^0 = a \\
&\mathrm{I}_i^k = f_i(\mathrm{I}^{k-1}) && \textit{if } i \in J^k \\
&\mathrm{I}_i^k = \mathrm{I}^{k-1} && \textit{if } i \notin J^k \\
&\mathrm{I}^\lambda = \sqcup_{k<\lambda} I^k
\end{aligned}$$

Theorem 11.11

$(\mathrm{I}^k, k < \lambda)$ *is increasing chain, ultimately stationary, and limit is* $lfp_a(f)$

Example: asynchronous iterations

- Jacobi iterations: $J^k = [1, n]$
  - update every component in each step
- Gauss-Seidel iterations: $J^k = \{k \ mod \ n\}$
  - update only one component in each step

End of Lecture 11