Formale Spezifikation und Verifikation

Mirco Tribastone

Institut für Informatik
Ludwig-Maximilians-Universität München
tribastone@pst.ifi.lmu.de

Fixed-Point Theory

Overview

- Preliminaries
- Tarski's fixed point theorem
- Application to strong bisimilarity

Preliminaries

Posets

Let D be a set. The pair $(D, \sqsubseteq)$ is called a *partially ordered set* (poset) iff $\sqsubseteq$ is a binary relation over D such that:

- $\sqsubseteq$ is reflexive, i.e., for any $d \in D$ it holds that $d \sqsubseteq d$;
- $\sqsubseteq$ is antisymmetric, i.e., for any $d, d' \in D$ if $d \sqsubseteq d'$ and $d' \sqsubseteq d$ then $d = d'$;
- $\sqsubseteq$ is transitive, i.e., for any $d, d', d'' \in D$ if $d \sqsubseteq d'$ and $d' \sqsubseteq d''$ then $d \sqsubseteq d''$.

For instance,

- $(\mathbb{N}, \leq)$, where $\mathbb{N}$ is the set of the naturals and $\leq$ is the standard less-or-equal relation, is a poset.
- $(\mathbb{R}, \leq)$, where $\mathbb{R}$ is the set of the reals, is a poset.
- Let S be a set. Then $(2^S, \subseteq)$ is a poset.

Bounds

Let $(D, \sqsubseteq)$ be a poset and $X \subseteq D$.

Upper bounds

$d \in D$ is said to be an *upper bound* for X iff $x \sqsubseteq d$ for all $x \in X$.

We say that d is the *least upper bound* (lub) for X, denoted by $\bigsqcup X$, iff the following conditions hold

- d is an upper bound for X;
- for any d' upper bound for X it holds that $d \sqsubseteq d'$.

Lower bounds

$d \in D$ is said to be a *lower bound* for X iff $d \sqsubseteq x$ for all $x \in X$.

We say that d is the *greatest lower bound* (glb) for X, denoted by $\bigsqcap X$, iff the following conditions hold

- d is a lower bound for X;
- for any d' lower bound for X it holds that $d' \sqsubseteq d$.

Examples

- In the poset $(\mathbb{N}, \leq)$ all finite subsets have least upper bounds, which correspond to their largest elements. Infinite subsets do not have upper bounds, i.e. $\{n \in \mathbb{N} \mid n > k\}$ for some $k \in \mathbb{N}$. However this set has the greatest lower bound: which one?
- In the poset $(2^S, \subseteq)$ every $X \subseteq 2^S$ (i.e., a collection of subsets of S) has an lub and glb, corresponding to $\bigcup X$ and $\bigcap X$, respectively.

Theorem (Uniqueness)

Let $(D, \sqsubseteq)$ be a poset and $X \subseteq D$. If an lub and a glb exist for X, they are unique.

Proof.

Uniqueness of glb Assume toward a contradiction that d and d' are two distinct glbs. Since they are also lower bounds, it must hold that $d \sqsubseteq d'$ and $d' \sqsubseteq d$. But due to antisymmetry this means that $d = d'$. □

Further Definitions

Complete Lattices

A poset $(D, \sqsubseteq)$ is said to be a *complete lattice* iff $\bigsqcup X$ and $\bigsqcap X$ exist for every $X \subseteq D$.

A complete lattice has a least element, denoted by $\bot = \bigsqcap D$ (bottom), and a top element $\top = \bigsqcup D$.

- The poset $(\mathbb{N}, \leq)$ is not a complete lattice, as discussed before.
- The poset $(2^S, \subseteq)$ is a complete lattice, with $\bot = \emptyset$ and $\top = S$.

Further Definitions

Monotonic Functions

Let $(D, \sqsubseteq)$ be a poset. A function $f : D \to D$ is *monotonic* iff $d \sqsubseteq d'$ implies $f(d) \sqsubseteq f(d')$ for any $d, d' \in D$.

Fixed points

Let $(D, \sqsubseteq)$ be a poset and $f : D \to D$ a monotonic function.
An element $d \in D$ is said to be a *fixed point* iff $d = f(d)$.

For instance, take the poset $(2^{\mathbb{N}}, \subseteq)$ and $f : 2^{\mathbb{N}} \to 2^{\mathbb{N}}$ as follows:

$$f(X) = X \cup \{1, 2\}.$$

f is monotonic and $A = \{1, 2\}$ is a fixed point because

$$f(A) = \{1, 2\} \cup \{1, 2\} = A\,.$$

A is not the only fixed point. Indeed, any B such that $A \subseteq B$ (e.g., $B = \{1, 2, 3\}$) is a fixed point also.

Tarski's Fixed Point Theorem

Theorem

Let $(D, \sqsubseteq)$ be a complete lattice and let $f : D \to D$ be monotonic. Then f has a largest fixed point, z_{max}, and a least fixed point, z_{min}, given by

$$z_{max} = \bigsqcup \{x \in D \mid x \sqsubseteq f(x)\} ,$$

$$z_{min} = \bigsqcap \{x \in D \mid f(x) \sqsubseteq x\} .$$

Proof.

(on blackboard)

□

Examples of Fixed Points

Consider the complete lattice $(2^S, \subseteq)$ for some set S, and a monotonic function $f : 2^S \to 2^S$. The statement of Tarski's theorem then reads

$$z_{max} = \bigcup \{ \underbrace{X \subseteq S}_{\text{i.e., } X \in 2^S} \mid X \subseteq f(X) \} ,$$

$$z_{min} = \bigcap \{ X \subseteq S \mid f(X) \subseteq X \} .$$

In particular, for $(2^{\mathbb{N}}, \subseteq)$ and $f(X) = X \cup \{1, 2\}, X \subseteq \mathbb{N}$ we have that

$$z_{max} = \bigcup \{ X \subseteq \mathbb{N} \mid X \subseteq X \cup \{1, 2\} \} = \mathbb{N} ,$$

$$z_{min} = \bigcap \{ X \subseteq \mathbb{N} \mid X \cup \{1, 2\} \subseteq X \} = \{1, 2\} .$$

How to algorithmically compute z_{max} and z_{min}?

Computing Fixed Points

Definition

Let D be a set, $d \in D$ and $f : D \to D$. For each natural n, $f^n(d)$ is defined as follows:

$$f^0(d) = d \qquad \text{and} \qquad f^{n+1}(d) = f(f^n(d)) \ .$$

Theorem

Let $(D, \sqsubseteq)$ a finite complete lattice and let $f : D \to D$ be monotonic. Then the least fixed point for f is computed as

$$z_{min} = f^m(\bot) \ ,$$

for some natural m. The largest fixed point is computed as

$$z_{max} = f^M(\top)$$

for some natural M.

Example

Consider the set $S = \{0, 1, 2\}$, the poset $(2^S, \subseteq)$, and the monotonic function $f : 2^S \to 2^S$ defined by

$$f(X) = (X \cap \{1\}) \cup \{2\} \ .$$

Recalling that $\bot = \emptyset$ and $\top = S$, the least fixed point is $\{2\}$ since

$$\begin{aligned} f^0(\bot) &= \emptyset \ , \\ f^1(\bot) &= f(\emptyset) = \{2\} \ , \\ f^2(\bot) &= f(\{2\}) = \{2\} = f^1(\bot) \ . \end{aligned}$$

The largest fixed point is $\{1, 2\}$ since

$$\begin{aligned} f^0(\top) &= \{0, 1, 2\} \ , \\ f^1(\top) &= f(\{0, 1, 2\}) = \{1, 2\} \ , \\ f^2(\top) &= f(\{1, 2\}) = \{1, 2\} = f^1(\top) \ . \end{aligned}$$

Bisimulation: Original Definitions

Strong Bisimulation

Let $(Q, A, \{\xrightarrow{a} \mid a \in A\})$ be an LTS. A relation $R \subseteq Q \times Q$ is *strong bisimulation* if, for any pair of states p and q such that $(p, q) \in R$, the following hold:

1. for all $a \in A$ and $p' \in Q$, if $p \xrightarrow{a} p'$ then $q \xrightarrow{a} q'$ for some $q' \in Q$ such that $(p', q') \in R$;
2. for all $a \in A$ and $q' \in Q$, if $q \xrightarrow{a} q'$ then $p \xrightarrow{a} p'$ for some $p' \in Q$ such that $(p', q') \in R$.

Bisimilarity

Two states $p, q \in Q$ are strongly *bisimilar*, written $p \sim q$, if there exists a strong bisimulation R such that $(p, q) \in R$.

$$\sim \; = \bigcup \{R \mid R \text{ is a strong bisimulation}\}$$

Fixed-Point Theory for Bisimulation

- Given an LTS $(Q, A, \{\xrightarrow{a} \mid a \in A\})$, where Q is finite, take $S = Q \times Q$ and consider the poset $\left(2^S, \subseteq\right)$
- A strong bisimulation R is therefore an element of 2^S.
- Consider now the set $\bigcup\{R \mid R \text{ is a strong bisimulation}\}$.
  It can be shown that the following equalities hold

  $$\sim = \bigcup\{R \mid R \text{ is a strong bisimulation}\} = \bigcup\left\{R \in 2^S \mid R \subseteq \mathcal{F}(R)\right\}$$

  if $\mathcal{F} : 2^S \to 2^S$ is defined as follows:

  $(p, q) \in \mathcal{F}(R)$ for all $p, q \in Q$ iff

  - $p \xrightarrow{a} p'$ implies $q \xrightarrow{a} q'$ for some q' such that $(p', q') \in R$;
  - $q \xrightarrow{a} q'$ implies $p \xrightarrow{a} p'$ for some p' such that $(p', q') \in R$.
- $\mathcal{F}$ can be shown to be monotonic. Thus, $\sim$ corresponds to the largest fixed point of $\mathcal{F}$, which is equal to $\mathcal{F}^M(\top) = \mathcal{F}^M(Q \times Q)$.

Example

$$Q_1 \triangleq b.Q_2 + a.Q_3$$
$$Q_2 \triangleq c.Q_4$$
$$Q_3 \triangleq c.Q_4$$
$$Q_4 \triangleq b.Q_2 + a.Q_3 + a.Q_1$$

Before, in order to construct $\sim$ we would consider that $Q_i \sim Q_i$, with $1 \leq i \leq 4$. Then we would check whether $Q_i \sim Q_j$, for all possible $i \neq j$, using the bisimulation game (and noticing that $Q_i \sim Q_j \iff Q_j \sim Q_i$).

For instance, to show that $Q_1 \not\sim Q_4$:

1. (Q_1, Q_4) **A:** $Q_4 \xrightarrow{a} Q_1$ **D:** $Q_1 \xrightarrow{a} Q_3$
2. (Q_3, Q_1) **A:** $Q_3 \xrightarrow{c} Q_4$ **D:** $Q_1 \not\xrightarrow{c}$

Example

$$Q_1 \triangleq b.Q_2 + a.Q_3$$
$$Q_2 \triangleq c.Q_4$$
$$Q_3 \triangleq c.Q_4$$
$$Q_4 \triangleq b.Q_2 + a.Q_3 + a.Q_1$$

Now, let $I = \{(Q_i, Q_i) \in Proc \times Proc \mid 1 \leq i \leq 4\}$. We have that:

$$\mathcal{F}^0(\top) = \mathcal{F}^0(Proc \times Proc) = Proc \times Proc$$
$$\mathcal{F}^1(\top) = \mathcal{F}(Proc \times Proc) = \{(Q_1, Q_4), (Q_4, Q_1), (Q_2, Q_3), (Q_3, Q_2)\} \cup I$$
$$\mathcal{F}^2(\top) = \{(Q_2, Q_3), (Q_3, Q_2)\} \cup I$$
$$\mathcal{F}^3(\top) = \{(Q_2, Q_3), (Q_3, Q_2)\} \cup I = \mathcal{F}^2(\top)$$