A Note on Complete Lattices and Tarski's Fixed Point Theorem

Luca Aceto, Anna Ingólfsdóttir and Kim G. Larsen
Department of Computer Science, Aalborg University
9220 Aalborg Ø, Denmark

March 3, 2003

1 Introduction

The aim of this note is to collect under one roof all the mathematical notions from the theory of partially ordered sets and lattices that is needed to introduce Tarski's classic fixed point theorem. We shall then use this theorem to give an alternative definition of strong bisimulation equivalence (also known as "strong equality"). This reformulation of the notion of strong bisimulation equivalence yields an algorithm for computing the largest strong bisimulation over finite labelled transition systems—i.e., labelled transition systems with only finitely many states and transitions.

The note is organized as follows. Section 2 introduces partially ordered sets and complete lattices. We then proceed to state and prove Tarski's fixed point theorem (Section 3). Finally, we show in Section 4 how to define strong bisimulation equivalence using Tarski's fixed point theorem, and hint at the algorithm for computing strong bisimulation equivalence over finite labelled transition systems that results from this reformulation.

2 Complete Lattices

Definition 2.1 [Partially Ordered Sets] A *partially ordered set (poset)* is a pair $(D, \sqsubseteq)$, where D is a set, and $\sqsubseteq$ is a binary relation over D (i.e, a subset of $D \times D$) such that:

- $\sqsubseteq$ is *reflexive*, i.e, $d \sqsubseteq d$ for all $d \in D$;
- $\sqsubseteq$ is *antisymmetric*, i.e, $d \sqsubseteq e$ and $e \sqsubseteq d$ imply $d = e$ for all $d, e \in D$;
- $\sqsubseteq$ is *transitive*, i.e, $d \sqsubseteq e \sqsubseteq d'$ implies $d \sqsubseteq d'$ for all $d, d', e \in D$.

We say that $(D, \sqsubseteq)$ is a *totally ordered set* if, for all $d, e \in D$, either $d \sqsubseteq e$ or $e \sqsubseteq d$ holds. $\square$

Example 2.2 The following are examples of posets:

- $(\mathbb{N}, \leq)$, where $\mathbb{N}$ denotes the set of natural numbers, and $\leq$ stands for the standard ordering over $\mathbb{N}$.
- $(A^*, \leq)$, where A^* is the set of strings over alphabet A, and $\leq$ denotes the prefix ordering between strings, i.e., for all $s, t \in A^*$, $s \leq t$ iff there exists $w \in A^*$ such that $sw = t$. (Check that this is indeed a poset!)
- Let $(A, \leq)$ be a finite totally ordered set. Then the set of strings in A^* ordered lexicographically is a poset. Recall that, for all $s, t \in A^*$, the relation $s \prec t$ holds with respect to the lexicographic order if:
  1. the length of s is smaller than that of t, or
  2. s and t have equal length, and there are strings $u, v, z \in A^*$ and letters $a, b \in A$ such that $s = uav$, $t = ubz$ and $a \leq b$.
- For each set S, the structure $(\mathcal{P}(S), \subseteq)$ is a poset, where $\mathcal{P}(S)$ stands for the set of all subsets of S.

Exercise 2.3 Which of the above posets is a totally ordered set?

Definition 2.4 [Least Upper Bounds and Greatest Lower Bounds] Let $(D, \sqsubseteq)$ be a poset, and take $X \subseteq D$.

- We say that $d \in D$ is an *upper bound* for X iff $x \sqsubseteq d$ for all $x \in X$. We say that d is the *least upper bound (lub)* of X, notation $\bigsqcup X$, iff d is an upper bound for X and, moreover, $d \sqsubseteq d'$ for every $d' \in D$ which is an upper bound for X.
- We say that $d \in D$ is a *lower bound* for X iff $d \sqsubseteq x$ for all $x \in X$. We say that d is the *greatest lower bound (glb)* of X, notation $\bigsqcap X$, iff d is a lower bound for X and, moreover, $d' \sqsubseteq d$ for every $d' \in D$ which is a lower bound for X.

□

Exercise 2.5 Let $(D, \sqsubseteq)$ be a poset, and take $X \subseteq D$. Prove that the lub and the glb of X are unique, if they exist.

Example 2.6

- In the poset $(\mathbb{N}, \leq)$, all finite subsets of $\mathbb{N}$ have least upper bounds. On the other hand, no infinite subset of $\mathbb{N}$ has an upper bound. All subsets of $\mathbb{N}$ have a least element, which is their greatest lower bound.
- In $(\mathcal{P}(S), \subseteq)$, *every* subset X of $\mathcal{P}(S)$ has a lub and a glb given by $\bigcup X$ and $\bigcap X$, respectively.

Exercise 2.7

1. Prove that the lub and the glb of a subset X of $\mathcal{P}(S)$ are indeed $\bigcup X$ and $\bigcap X$, respectively.

2. Give examples of subsets of A^* that have upper bounds in the poset $(A^*, \leq)$.

Definition 2.8 [Complete Lattices] A poset $(D, \sqsubseteq)$ is a *complete lattice* iff $\bigsqcup X$ and $\bigsqcap X$ exist for every subset X of D. $\square$

Note that a complete lattice $(D, \sqsubseteq)$ has a least element $\bot = \bigsqcap D$, and a top element $\top = \bigsqcup D$.

Exercise 2.9 Let $(D, \sqsubseteq)$ be a complete lattice. What are $\bigsqcup \emptyset$ and $\bigsqcap \emptyset$?

Example 2.10

- The poset $(\mathbb{N}, \leq)$ is *not* a complete lattice because, as remarked previously, it does not have lub's for its infinite subset.

- The poset $(\mathbb{N} \cup \{\infty\}, \sqsubseteq)$, obtained by adding a largest element ∞ to $(\mathbb{N}, \leq)$, is a complete lattice. This complete lattice can be pictured as follows:

$$\begin{array}{c} \infty \\ \vdots \\ \uparrow \\ 2 \\ \uparrow \\ 1 \\ \uparrow \\ 0 \end{array}$$

- $(\mathcal{P}(S), \subseteq)$ is a complete lattice.

3 Tarski's Fixed Point Theorem

Definition 3.1 [Monotonic Functions and Fixed Points] Let $(D, \sqsubseteq)$ be a poset. A function $f : D \to D$ is *monotonic* iff for all $d, d' \in D$, $d \sqsubseteq d'$ implies that $f(d) \sqsubseteq f(d')$.

An element $d \in D$ is called a *fixed point* of f iff $d = f(d)$. $\square$

The following important theorem is due to Tarski [3], and was also independently proven by Knäster.

Theorem 3.2 (Tarski's Fixed Point 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:*

$$\begin{aligned} z_{\max} &= \bigsqcup \{x \in D \mid x \sqsubseteq f(x)\} \\ z_{\min} &= \bigsqcap \{x \in D \mid f(x) \sqsubseteq x\} \end{aligned}$$

Proof: First we shall prove that $z_{\max}$ is the largest fixed point of f. This involves proving the following two statements:

1. $z_{\max}$ is a fixed point of f, i.e., $z_{\max} = f(z_{\max})$, and
2. for every $d \in D$ that is a fixed point of f, it holds that $d \sqsubseteq z_{\max}$.

In what follows we prove each of these statements separately. In the rest of the proof we let

$$A = \{x \in D \mid x \sqsubseteq f(x)\}.$$

1. To prove that $z_{\max}$ is a fixed-point of f, it is sufficient to show that

   $$\begin{aligned} z_{\max} &\sqsubseteq f(z_{\max}) \quad \text{and} & (1) \\ f(z_{\max}) &\sqsubseteq z_{\max}. & (2) \end{aligned}$$

   First of all, we shall show that (1) holds. By definition, we have that

   $$z_{\max} = \bigsqcup A.$$

   Thus, for every $x \in A$, it holds that $x \sqsubseteq z_{\max}$. As f is monotonic, $x \sqsubseteq z_{\max}$ implies that $f(x) \sqsubseteq f(z_{\max})$. It follows that, for every $x \in A$, $x \sqsubseteq f(x) \sqsubseteq f(z_{\max})$. Thus $f(z_{\max})$ is an upper bound for the set A. By definition, $z_{\max}$ is the *least upper bound* of A. Thus $z_{\max} \sqsubseteq f(z_{\max})$, and we have shown (1).

   To prove that (2) holds, note that, from (1) and the monotonicity of f, we have that $f(z_{\max}) \sqsubseteq f(f(z_{\max}))$. This implies that $f(z_{\max}) \in A$. Therefore $f(z_{\max}) \sqsubseteq z_{\max}$, as $z_{\max}$ is an upper bound for A.

   From (1) and (2), we have that $z_{\max} \sqsubseteq f(z_{\max}) \sqsubseteq z_{\max}$. By antisymmetry, it follows that $z_{\max} = f(z_{\max})$, i.e., $z_{\max}$ is a fixed point of f.

2. We now show that $z_{\max}$ is the largest fixed point of f. Let d be any fixed point of f. Then, in particular, we have that $d \sqsubseteq f(d)$. This implies that $d \in A$ and therefore that $d \sqsubseteq \bigsqcup A = z_{\max}$.

   We have thus shown that $z_{\max}$ is the largest fixed point of f.

To show that $z_{\min}$ is the least fixed point of f, we proceed in a similar fashion by proving the following two statements:

1. $z_{\min}$ is a fixed point of f, i.e., $z_{\min} = f(z_{\min})$, and
2. for every $d \in D$ that is a fixed point of f, $z_{\min} \sqsubseteq d$.

To prove that $z_{\min}$ is a fixed point of f, it is sufficient to show that:

$$\begin{aligned} f(z_{\min}) &\sqsubseteq z_{\min} \quad \text{and} && (3) \\ z_{\min} &\sqsubseteq f(z_{\min}). && (4) \end{aligned}$$

Claim (3) can be shown following the proof for (1), and claim (4) can be shown following the proof for (2). The details are left as an exercise for the reader. Having shown that $z_{\min}$ is a fixed point of f, it is a simple matter to prove that it is indeed the least fixed point of f. (Do this as an exercise). □

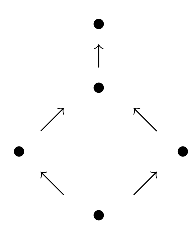
Exercise 3.3

1. Prove that if $(D, \sqsubseteq)$ is a cpo and $f : D \to D$ is continuous (see [2, Page 103]), then the poset

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

   which consists of the set of fixed points of f is a cpo.

2. Give an example of a complete lattice $(D, \sqsubseteq)$ and of a monotonic function $f : D \to D$ such that there are $x, y \in D$ that are fixed points of f, but $\bigsqcup\{x, y\}$ is *not* a fixed point. [*Hint*: Consider the complete lattice D pictured below

   and construct such an $f : D \to D$.]

3. Let $(D, \sqsubseteq)$ be a complete lattice, and let $f : D \to D$ be monotonic. Consider a subset X of $\{x \in D \mid x \sqsubseteq f(x)\}$.
   (a) Prove that $\bigsqcup X \in \{x \in D \mid x \sqsubseteq f(x)\}$.
   (b) Give an example showing that, in general, $\bigsqcap X \notin \{x \in D \mid x \sqsubseteq f(x)\}$. [*Hint*: Consider the lattice pictured above turned upside down.]

4. Let $(D, \sqsubseteq)$ be a complete lattice, and let $f : D \to D$ be monotonic. Consider a subset X of $\{x \in D \mid f(x) \sqsubseteq x\}$.

(a) Prove that $\bigsqcap X \in \{x \in D \mid f(x) \sqsubseteq x\}$.

(b) Give an example showing that, in general, $\bigsqcup X \notin \{x \in D \mid f(x) \sqsubseteq x\}$. [*Hint*: Use your solution to exercise 2 above.]

5. Let $(D, \sqsubseteq)$ be a complete lattice.

(a) Let $D \rightarrow_{mon} D$ be the set of monotonic functions from D to D and $\preceq$ be the relation defined on $D \rightarrow_{mon} D$ by

$$f \preceq g \text{ iff } \forall d \in D.\ f(d) \sqsubseteq g(d).$$

Show that $\preceq$ is a partial order on $D \rightarrow_{mon} D$.

(b) Let $\bigvee$ and $\bigwedge$ be defined on $D \rightarrow_{mon} D$ by:

$$\text{If } \mathcal{F} \subseteq D \rightarrow_{mon} D \text{ then } \forall d \in D.(\bigvee \mathcal{F})(d) = \bigsqcup\{f(d) | f \in \mathcal{F}\}$$

and

$$\text{If } \mathcal{F} \subseteq D \rightarrow_{mon} D \text{ then } \forall d \in D.(\bigwedge \mathcal{F})(d) = \bigsqcap\{f(d) | f \in \mathcal{F}\}.$$

Show that $(D \rightarrow_{mon} D, \preceq)$ is a complete lattice with $\bigvee$ and $\bigwedge$ as lub and glb.

The following theorem gives a characterization of the greatest and least fixed points for monotonic functions over *finite* complete lattices.

Theorem 3.4 *Let $(D, \sqsubseteq)$ be a* finite *complete lattice and let $f : D \rightarrow D$ be monotonic. Then the least fixed point for f is obtained as*

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

for some m, where $f^0(\bot) = \bot$, and $f^{n+1}(\bot) = f(f^n(\bot))$. Furthermore the greatest fixed point for f is obtained as

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

for some M, where $f^0(\top) = \top$, and $f^{n+1}(\top) = f(f^n(\top))$.

Proof: We only prove the first statement as the proof for the second one is similar. As f is monotonic we have the following non-decreasing sequence

$$\bot \sqsubseteq f(\bot) \sqsubseteq f^2(\bot) \sqsubseteq \ldots \sqsubseteq f^i(\bot) \sqsubseteq f^{i+1}(\bot) \sqsubseteq \ldots$$

of elements of D. As D is finite, the sequence must be eventually constant, i.e., there is an m such that $f^k(\bot) = f^m(\bot)$ for all $k \geq m$. In particular $f(f^m(\bot)) = f^{m+1}(\bot) = f^m(\bot)$ which is the same as saying that $f^m(\bot)$ is a fixed point for f.

To prove that $f^m(\bot)$ is the least fixed point for f, assume that d is another fixed point for f. Then we have that $\bot \sqsubseteq d$ and therefore, as f is monotonic, that $\bot \sqsubseteq f(\bot) \sqsubseteq f(d) = d$. By repeating this reasoning $m-1$ more times we get that $f^m(\bot) \sqsubseteq d$. We can therefore conclude that $f^m(\bot)$ is the least fixed point for f.

The proof of the statement that characterizes largest fixed points is similar, and left as an exercise for the reader. $\square$

4 Bisimulation as a Fixed Point

Let $(Proc, \mathsf{Act}, \longrightarrow)$ be a labelled transition system. We recall that a relation $S \subseteq Proc \times Proc$ is a *strong bisimulation* [1] if the following holds:

If $(p, q) \in S$ then, for every $\alpha \in \mathsf{Act}$:

1. $p \xrightarrow{\alpha} p'$ implies $q \xrightarrow{\alpha} q'$ for some q' such that $(p', q') \in S$.
2. $q \xrightarrow{\alpha} q'$ implies $p \xrightarrow{\alpha} p'$ for some p' such that $(p', q') \in S$.

Then *strong bisimulation equivalence* (or *strong equality*) is defined as

$$\sim \;\; = \;\; \bigcup \{S \in \mathcal{P}(Proc \times Proc) \mid S \text{ is a strong bisimulation}\}.$$

In what follows we shall describe the relation $\sim$ as a fixed point to a suitable monotonic function. First we note that $(\mathcal{P}(Proc \times Proc), \subseteq)$ (i.e., the set of binary relations over $Proc$ ordered by set inclusion) is a complete lattice with $\bigcup$ and $\bigcap$ as the lub and glb. (Check this!) Next we define a function $\mathcal{F} : \mathcal{P}(Proc \times Proc) \longrightarrow \mathcal{P}(Proc \times Proc)$ as follows.

$(p, q) \in \mathcal{F}(S)$ if and only if:

1. $p \xrightarrow{\alpha} p'$ implies $q \xrightarrow{\alpha} q'$ for some q' such that $(p', q') \in S$.
2. $q \xrightarrow{\alpha} q'$ implies $p \xrightarrow{\alpha} p'$ for some p' such that $(p', q') \in S$.

Then S is a bisimulation if and only if $S \subseteq \mathcal{F}(S)$ and consequently

$$\sim \;\; = \;\; \bigcup \{S \in \mathcal{P}(Proc \times Proc) \mid S \subseteq \mathcal{F}(S)\}.$$

We note that if $S, R \in \mathcal{P}(Proc \times Proc)$ and $S \subseteq R$ then $\mathcal{F}(S) \subseteq \mathcal{F}(R)$ (check this!), i.e., $\mathcal{F}$ is monotonic over $(\mathcal{P}(Proc \times Proc), \subseteq)$. Therefore, as all the conditions for Tarski's Theorem are satisfied, we can conclude that $\sim$ is the greatest fixed point of $\mathcal{F}$. In particular, by Theorem 3.4, if $Proc$ is finite then $\sim$ is equal to $\mathcal{F}^M(Proc \times Proc)$ for some $M \geq 0$. Note how this gives us an algorithm to calculate $\sim$ for a given finite labelled transition system: To compute $\sim$, simply evaluate the non-increasing sequence $\mathcal{F}^i(Proc \times Proc)$ for $i \geq 0$ until the sequence stabilizes.

Example 4.1 Consider the labelled transition system described by the following equations:

$$\begin{aligned} Q_1 &= b.Q_2 + a.Q_3 \\ Q_2 &= c.Q_4 \\ Q_3 &= c.Q_4 \\ Q_4 &= b.Q_2 + a.Q_3 + a.Q_1 \ . \end{aligned}$$

In this labelled transition system, we have that

$$Proc = \{Q_i \mid 1 \leq i \leq 4\} \ .$$

Below, we use I to denote the identity relation over $Proc$—that is,

$$I = \{(Q_i, Q_i) \mid 1 \leq i \leq 4\} \ .$$

We calculate the sequence $\mathcal{F}^i(Proc \times Proc)$ for $i \geq 1$ thus:

$$\begin{aligned} \mathcal{F}^1(Proc \times Proc) &= \{(Q_1, Q_4), (Q_4, Q_1), (Q_2, Q_3), (Q_3, Q_2)\} \cup I \\ \mathcal{F}^2(Proc \times Proc) &= \{(Q_2, Q_3), (Q_3, Q_2)\} \cup I \quad \text{and finally} \\ \mathcal{F}^3(Proc \times Proc) &= \mathcal{F}^2(Proc \times Proc) \ . \end{aligned}$$

Therefore, the only distinct processes that are related by the largest strong bisimulation over this labelled transition system are Q_2 and Q_3.

Exercise 4.2

1. Using the iterative algorithm described above, compute the largest strong bisimulation over the following transition system:

$$\begin{aligned} P_1 &= a.P_2 \\ P_2 &= a.P_1 \\ P_3 &= a.P_2 + a.P_4 \\ P_4 &= a.P_3 + a.P_5 \\ P_5 &= 0 \ . \end{aligned}$$

2. What is the worst case complexity of the algorithm outlined above when run on a labelled transition system consisting of n states and m transitions?

3. Give a similar characterization for observational equivalence as a fixed point for a monotonic function.

References

[1] R. Milner. *Communication and Concurrency.* Prentice-Hall, Englewood Cliffs, 1989.

[2] H.R. Nielson and F. Nielson. *Semantics with Applications: A Formal Introduction*. Wiley Professional Computing. John Wiley & Sons, Chichester, England, 1992.

[3] A. Tarski. A lattice-theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics*, 5, pp. 285–309, 1955.