Lattices and the Knaster-Tarski Theorem

Deepak D’Souza

Department of Computer Science and Automation
Indian Institute of Science, Bangalore.

8 August 2017
Outline

1. Why study lattices
2. Partial Orders
3. Lattices
4. Knaster-Tarski Theorem
5. Computing LFP
What a lattice looks like

Subsets of \( \{1, 2, 3\} \),

“subset”

Odd/even, “contained in”
Why study lattices in program analysis?

Why lattices?

- Natural way to obtain the “collecting state” at a point is to take union of states reached along each path leading to the point.
- With abstract states also we want a “union” or “join” over all paths (JOP).

Why fixpoints?

- Guaranteed to safely approximate JOP (* Conditions apply).
- Easier to compute than JOP.
- Knaster-Tarski theorem tells us when a fixpoint exists and what it looks like.

```latex
1: p = 5;
2: q = 2;
3: while (p > q) {
   4: p := p+1;
   5: q := q+2;
}
6: print p;
```
Partial Orders

- Usual order (or total order) on numbers: $1 \leq 2 \leq 3$.
- Some domains are naturally “partially” ordered:

Subsets of $\{1, 2, 3\}$, “subset”

Divisors of 12, “divides”

Odd/even, “contained in”
A partially ordered set is a non-empty set $D$ along with a partial order $\leq$ on $D$. Thus $\leq$ is a binary relation on $D$ satisfying:

- $\leq$ is reflexive ($d \leq d$ for each $d \in D$)
- $\leq$ is transitive ($d \leq d'$ and $d' \leq d''$ implies $d \leq d''$)
- $\leq$ is anti-symmetric ($d \leq d'$ and $d' \leq d$ implies $d = d'$).
We can view a binary relation on a set as a directed graph. For example, the binary relation

\[ \{(a, a), (a, b), (b, c), (b, e), (d, e), (d, c), (e, f)\} \]

can be represented as the graph:
A partial order is then a special kind of directed graph:

- Reflexive = self-loop on each node
- Antisymmetric = no 2-length cycles
- Transitive = “transitivity” of edges.

Graph representation

Hasse-diagram representation
Upper bounds etc.

In a partially ordered set \((D, \leq)\):

- An element \(u \in D\) is an upper bound of a set of elements \(X \subseteq D\), if \(x \leq u\) for all \(x \in X\).
- \(u\) is the least upper bound (or lub or join) of \(X\) if \(u\) is an upper bound for \(X\), and for every upper bound \(y\) of \(X\), we have \(u \leq y\). We write \(u = \bigvee X\).
- Similarly, \(v = \bigwedge X\) (\(v\) is the greatest lower bound or glb or meet of \(X\)).
A **lattice** is a partially order set in which every pair of elements has an lub and a glb.

A **complete** lattice is a lattice in which every *subset* of elements has a lub and glb.
A **lattice** is a partially order set in which every pair of elements has an lub and a glb.

A **complete** lattice is a lattice in which every *subset* of elements has a lub and glb.

Examples below are all complete lattices.
More lattices
Exercise

1. Example of a partial order that is not a lattice?
Exercise

1. Example of a partial order that is not a lattice?
Exercise

1. Example of a partial order that is not a lattice?

2. “Simplest” example of a partial order that is not a lattice?
Exercise

1. Example of a partial order that is not a lattice?

   \[
   \begin{array}{ccc}
   & d & \\
   a & & c \\
   & b & \\
   \end{array}
   \]

2. “Simplest” example of a partial order that is not a lattice?

   \[
   \begin{array}{ccc}
   a & & b \\
   \end{array}
   \]
Exercise

1. Example of a partial order that is not a lattice?
   ![Graph](image)

2. “Simplest” example of a partial order that is not a lattice?
   ![Graph](image)

3. Example of a lattice which is not complete?
Exercise

1. Example of a partial order that is not a lattice?

   ![Diagram of a partial order that is not a lattice]

2. “Simplest” example of a partial order that is not a lattice?

   ![Diagram of a partial order that is not a lattice]

3. Example of a lattice which is not complete?

   ![Diagram of a lattice which is not complete]
Let \((D, \leq)\) be a partially ordered set.

- A function \(f : D \rightarrow D\) is **monotonic** or **order-preserving** if whenever \(x \leq y\) we have \(f(x) \leq f(y)\).
Partial order induced by a subset of elements

Let \((D, \leq)\) be a partially ordered set, and \(X\) be a non-empty subset of \(D\). Then \(X\) induces a partial order, which we call the partial order \textit{induced by} \(X\) in \((D, \leq)\), and defined to be \((X, \leq \cap (X \times X))\).

Example: the partial order induced by the set of elements \(X = \{2, 3, 12\}\).
A **fixpoint** of a function $f : D \to D$ is an element $x \in D$ such that $f(x) = x$.

A **pre-fixpoint** of $f$ is an element $x$ such that $x \leq f(x)$.

A **post-fixpoint** of $f$ is an element $x$ such that $f(x) \leq x$. 

---

Why study lattices

Partial Orders

Lattices

Knaster-Tarski Theorem

Computing LFP
Knaster-Tarski Fixpoint Theorem

Theorem (Knaster-Tarski)

Let $(D, \leq)$ be a complete lattice, and $f : D \rightarrow D$ a monotonic function on $(D, \leq)$. Then:

(a) $f$ has at least one fixpoint.

(b) $f$ has a least fixpoint which coincides with the glb of the set of postfixpoints of $f$, and a greatest fixpoint which coincides with the lub of the prefixpoints of $f$.

(c) The set of fixpoints $P$ of $f$ itself forms a complete lattice under $\leq$. 
Fixpoints of $f$

Stars denote fixpoints.
Exercise

Consider the complete lattice and monotone function $f$ below.

1. Mark the pre-fixpoints with up-triangles ($\triangle$).
2. What is the lub of the pre-fixpoints?
3. Mark post-fixpoints with down-triangles ($\nabla$).
4. Fixpoints are the stars ($\Box$).

Check that claims of K-T theorem hold here.
If you drop completeness of lattice or monotonicity of $f$, does K-T still hold?
Proof of Knaster-Tarski theorem

(a) $g = \bigcup Pre$ is a fixpoint of $f$.
(b) $g$ is the greatest fixpoint of $f$.
(c) Similarly $l = \bigcap Post$ is the least fixpoint of $f$.
(d) Let $P$ be the set of fixpoints of $f$. Then $(P, \leq)$ is a complete lattice.
Proof of K-T theorem: (a)
Proof of K-T theorem: (a)

To show $g = f(g)$:
Proof of K-T theorem: (a)

To show $g = f(g)$:

- $g \leq f(g)$
Proof of K-T theorem: (a)

To show $g = f(g)$:

- $g \leq f(g)$
- Since $f(g)$ can be seen to be u.b. of $Pre$. 
Proof of K-T theorem: (a)

To show $g = f(g)$:
- $g \leq f(g)$
- Since $f(g)$ can be seen to be u.b. of $Pre$.
- $f(g) \leq g$
Proof of K-T theorem: (a)

To show $g = f(g)$:

- $g \leq f(g)$
  - Since $f(g)$ can be seen to be u.b. of $Pre$.
- $f(g) \leq g$
  - Since $f(g)$ can be seen to be prefixpoint of $f$. 
Proof of K-T theorem: (b)

\( g \) is the greatest fixpoint of \( f \).
Proof of K-T theorem: (b)

\[ g \text{ is the greatest fixpoint of } f. \]

Any other fixpoint is also a pre-fixpoint of \( f \), and hence \( g \) must dominate it.
Exercise: intervals and closure

Let \((D, \leq)\) be a partial order, and let \(f : D \to D\).

- Let \(a, b \in D\). The interval from \(a\) to \(b\), written \([a, b]\), is the set \(\{d \mid a \leq d \leq b\}\).

- A subset \(X \subseteq D\) is said to be closed wrt to \(f\), if \(f(x) \in X\) for each \(x \in X\).

Exercise: Let \((D, \leq)\) be a partial order with a \(\top\) element, and let \(f : D \to D\) be a monotone function on \(D\).

1. Show that an interval in \(D\) need *not* be closed wrt \(f\).

2. Let \(u \in D\) be the lub of a set \(X\) of fixpoints of \(f\). Prove that the interval \([u, \top]\) is closed wrt \(f\).
Proof of K-T theorem: (d)

1. \((P, \leq)\) is also a partial order.
2. \((P, \leq)\) is a complete lattice
   - Let \(X \subseteq P\). We show there is an lub of \(X\) in \((P, \leq)\).
     - Let \(u\) be lub of \(X\) in \((D, \leq)\).
     - Consider “interval” \(I = [u, \top] = \{x \in D \mid u \leq x\}\).
     - \((I, \leq)\) is also a complete lattice.
     - \(f : I \rightarrow I\) as well, and monotonic on \((I, \leq)\).
     - Hence by part (a) \(f\) has a least fixpoint in \(I\), say \(v\).
     - Argue that \(v\) is the lub of \(X\) in \((P, \leq)\).
Chains in Partial Orders

- A **chain** in a partial order \((D, \leq)\) is a totally ordered subset of \(D\).
- An **ascending chain** is an infinite sequence of elements of \(D\) of the form:
  \[
  d_0 \leq d_1 \leq d_2 \leq \cdots
  \]
- An ascending chain \(\langle d_i \rangle\) is **eventually stable** if there exists \(n_0\) such that \(d_i = d_{n_0}\) for each \(i \geq n_0\).
- \((D, \leq)\) has **finite** height if each chain in it is finite.
- \((D, \leq)\) has **bounded** height if there exists \(k\) such that each chain in \(D\) has height at most \(k\) (i.e. number of elements in each chain is at most \(k + 1\)).
Monotonicity, distributivity, and continuity

- **f** is monotone:
  
  \[ x \leq y \implies f(x) \leq f(y). \]

- **f** is distributive:
  
  \[ f(x \sqcup y) = f(x) \sqcup f(y). \]

- **f** is continuous: For any asc chain \( X \):
  
  \[ f(\bigsqcup X) = \bigsqcup (f(X)). \]

- **f** is inf distributive: For any \( X \subseteq D \):
  
  \[ f(\bigsqcap X) = \bigsqcap (f(X)). \]
Characterising lfp’s and gfp’s of a function \( f \) in a complete lattice \((D, \leq)\)

- \( f \) is **continuous** if for any ascending chain \( X \) in \( D \),
  \[
  f(\bigsqcup X) = \bigsqcup (f(X)).
  \]

- If \( f \) is **continuous** then
  \[
  \text{lfp}(f) = \bigsqcup_{i \geq 0} (f^i(\bot)).
  \]

- If \( f \) is **monotonic** and \((D, \leq)\) has **finite height** then we can compute \( \text{lfp}(f) \) by finding the stable value of the asc. chain
  \[
  \bot \leq f(\bot) \leq f^2(\bot) \leq f^3(\bot) \leq \cdots.
  \]