Lecturecise 13
Abstract Interpretation

2013

Constructing Partial Orders using Maps

Example: Let A be the set of all propositional formulas containing only variables p, q. For a formula $F \in A$ define

$$[F] = \{(u, v).\ u, v \in \{0, 1\} \wedge F \text{ is true for } p \mapsto u, q \mapsto v\}$$

i.e. $[F]$ denotes the set of assignments for which F is true. Note that $F \implies G$ is a tautology iff $[F] \subseteq [G]$. Define ordering on formulas A by

$$F \leq G \iff [F] \subseteq [G]$$

Is $\leq$ a partial order? Which laws does $\leq$ satisfy?

Constructing Partial Orders using Maps

Lemma: Let $(C, \leq)$ be an lattice and A a set. Let $\gamma : A \to C$ be an injective function. Define oder $x \sqsubseteq y$ on A by $\gamma(x) \leq \gamma(y)$. Then $(A, \sqsubseteq)$ is a partial order.

Note: even if $(C, \leq)$ had top and bottom element and was a lattice, the constructed order need not have top and bottom or be a lattice. For example, we take A to be a subset of A and define γ to be identity.

Lattices

Definition: A lattice is a partial order in which every two-element set has a least upper bound and a greatest lower bound (so, we have $\sqcap$ and $\sqcup$ as well-defined binary operations).

Lemma: In every lattice, $x \sqcup (x \sqcap y) = x$.

Lattices

Definition: A lattice is a partial order in which every two-element set has a least upper bound and a greatest lower bound (so, we have $\sqcap$ and $\sqcup$ as well-defined binary operations).
Lemma: In every lattice, $x \sqcup (x \sqcap y) = x$.

Proof:
We trivially have $x \sqsubseteq x \sqcup (x \sqcap y)$.
Let's prove that $x \sqcup (x \sqcap y) \sqsubseteq x$:
x is an upper bound of x and $x \sqcap y$, $x \sqcup (x \sqcap y)$ is the least upper bound of x and $x \sqcap y$, thus $x \sqcup (x \sqcap y) \sqsubseteq x$.
Definition: A lattice is //distributive// iff

$$x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$$
$$x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$$

Lattice of all subsets of a set is distributive. Linear order is a distributive lattice.

Products of Lattices

Note: for $n = 2$ a function $f : \{1, 2\} \to (L_1 \cup L_2)$ with $f(1) \in L_1$, $f(2) \in L_2$ is isomorphic to an ordered pair $(f(1), f(2))$. We denote the product by $(L_1, \leq_1) \times (L_2, \leq_2)$.
Example: Let $R = \{a, b, c, d\}$ denote set of values. Let $A_1 = A_2 = 2^R$. Let

$$s_1 \leq_1 s_2 \iff s_1 \subseteq s_2$$

and let

$$t_1 \leq_2 t_2 \iff t_1 \supseteq t_2$$

Then we can define the product $(A_1, \leq_1) \times (A_2, \leq_2)$. In this product, $(s_1, t_1) \leq (s_2, t_2)$ iff: $s_1 \subseteq s_2$ and $t_1 \supseteq t_2$. The original partial orders were lattices, so the product is also a lattice. For example, we have

$$(\{a, b, c\}, \{a, b, d\}) \sqcap (\{b, c, d\}, \{c, d\}) = (\{b, c\}, \{a, b, c, d\})$$

Products of Lattices

Lattice elements can be combined into finite or infinite-dimensional vectors, and the result is again a lattice.

Lemma: Let $(A_1, \leq_1), \ldots, (A_n, \leq_n)$ be partial orders. Define $(L, \leq)$ by

$$A = \{f \mid f : \{1, \ldots, n\} \to (A_1 \cup \ldots \cup A_n) \text{ where } \forall i. f(i) \in A_i\}$$

For $f, g \in A$ define

$$f \leq g \iff \forall i. f(i) \leq_i g(i)$$

Then $(A, \leq)$ is a partial order. We denote $(A, \leq)$ by

$$\prod_{i=1}^{n} (L_i, \leq_i)$$

Moreover, if for each i, $(A_i, \leq_i)$ is a lattice, then $(A, \leq)$ is also a lattice.

Properties of $\sqcap S$ and $\sqcup S$

$\forall x.\ \bot \sqsubseteq x$

A is infinite

Consider a partial order $(A, \sqsubseteq)$.

- Suppose $S_1 \subseteq S_2 \subseteq A$ and $\sqcup S_1$ and $\sqcup S_2$ exist. In what relationship are these two elements? $\sqcup S_1 \sqsubseteq \sqcup S_2 \rightarrow \forall x \in S_1\ x \sqsubseteq \sqcup S_2$
- Suppose $S_1 \subseteq S_2 \subseteq A$ and $\sqcap S_1$ and $\sqcap S_2$ exist. In what relationship are these two elements? $\sqcap S_2 \sqsubseteq \sqcap S_1 \quad \forall y \in S_1\ \sqcap S_2 \sqsubseteq y$
- Suppose $\sqcup\emptyset$ exists. Describe this element. $\bot$
- Suppose $\sqcap\emptyset$ exists. Describe this element. $\top$

$\sqcup \emptyset = a$ $\qquad\qquad$ $\sqcup \emptyset = \bot$

$(\forall x \in \emptyset \quad x \sqsubseteq a) \qquad \forall x.\ x \in \emptyset \rightarrow \ldots$

$\forall b.\ \underbrace{(\forall x \in \emptyset\ x \sqsubseteq b)}_{\text{true.}} \rightarrow a \sqsubseteq b \qquad\qquad \forall b.\ a \sqsubseteq b$

Properties of $\sqcap S$ and $\sqcup S$

Consider a partial order $(A, \sqsubseteq)$.

- Suppose $S_1 \subseteq S_2 \subseteq A$ and $\sqcup S_1$ and $\sqcup S_2$ exist. In what relationship are these two elements?
- Suppose $S_1 \subseteq S_2 \subseteq A$ and $\sqcap S_1$ and $\sqcap S_2$ exist. In what relationship are these two elements?
- Suppose $\sqcup\emptyset$ exists. Describe this element.
- Suppose $\sqcap\emptyset$ exists. Describe this element.

$\sqcup\emptyset = \bot$ and $\sqcap\emptyset = \top$. This is because every element is an upper bound and a lower bound of $\emptyset$: $\forall x.\forall y \in \emptyset.y \sqsubseteq x$ is valid, as well as $\forall x.\forall y \in \emptyset.y \sqsupseteq x$.

Complete Semilattice is a Complete Lattice

If we have all $\sqcap$-s we then also have all $\sqcup$-s:

Theorem: Let $(A, \sqsubseteq)$ be a partial order such that every set $S \subseteq A$ has the greatest lower bound ($\sqcap$). Prove that then every set $S \subseteq A$ has the least upper bound ($\sqcup$).

Example: Application of the Previous Theorem

Let U be a set and $A \subseteq U \times U$ the set of all **equivalence relations** on this set. Consider the partial order $(A, \subseteq)$.

Lemma

If $I \subseteq A$ is a set of equivalence relations, then $\cap I$ is also an equivalence relation.

Consequence: Given $I \subseteq A$ there exists the least equivalence relation containing every relation from I (equivalence closure of relations in I).

Note: **congruence** is equivalence relation that agrees with some operations. For example, $x \sim x'$ and $y \sim y'$ implies $(x + y) \sim (x' + y')$. The analogous properties hold for congruence relations.

Complete Lattices

Definition: A **complete** lattice is a lattice where for every set S (including empty set and infinite sets) there exist $\sqcup S$ and $\sqcap S$.

Monotonic functions

Given two partial orders $(C, \leq)$ and $(A, \sqsubseteq)$, we call a function $\alpha : C \to A$ *monotonic* iff for all $x, y \in C$,

$$x \leq y \;\to\; \alpha(x) \sqsubseteq \alpha(y)$$

Reminder: Fixpoints

Definition: Given a set A and a function $f : A \to A$ we say that $x \in A$ is a fixed point (fixpoint) of f if $f(x) = x$.

Definition: Let $(A, \leq)$ be a partial order, let $f : A \to A$ be a monotonic function on $(A, \leq)$, and let the set of its fixpoints be $S = \{x \mid f(x) = x\}$. If the least element of S exists, it is called the **least fixpoint**, if the greatest element of S exists, it is called the **greatest fixpoint**.

Fixpoints

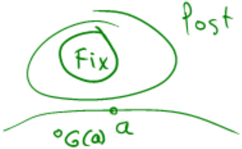
Let $(A, \sqsubseteq)$ be a complete lattice and $G : A \to A$ a monotonic function.

Definition:
Post $= \{x \mid G(x) \sqsubseteq x\}$ - the set of *postfix points* of G
(e.g. $\top$ is a postfix point)
Pre $= \{x \mid x \sqsubseteq G(x)\}$ - the set of *prefix points* of G
Fix $= \{x \mid G(x) = x\}$ - the set of *fixed points* of G.

Note that Fix $\subseteq$ Post.

Tarski's fixed point theorem

Theorem: Let $a = \sqcap\text{Post}$. Then a is the least element of Fix (dually, $\sqcup\text{Pre}$ is the largest element of Fix).



$\forall x \in \text{Post}$

$a \sqsubseteq x$

Proof: $G(x) \sqsubseteq x$

Let x range over elements of Post.

- applying monotonic G from $a \sqsubseteq x$ we get $G(a) \sqsubseteq G(x) \sqsubseteq x$
- so $G(a)$ is a lower bound on Post, but a is the greatest lower bound, so $G(a) \sqsubseteq a$
- therefore $a \in \text{Post}$

  $x \in \text{Post}$ $G(x) \sqsubseteq x$ / G

  $G(G(x)) \sqsubseteq G(x)$
- Post is closed under G, by monotonicity, so $G(a) \in \text{Post}$
- a is a lower bound on Post, so $a \sqsubseteq G(a)$
- from $a \sqsubseteq G(a)$ and $G(a) \sqsubseteq a$ we have $a = G(a)$, so $a \in \text{Fix}$
- a is a lower bound on Post so it is also a lower bound on a smaller set Fix

In fact, the set of all fixpoints Fix is a lattice itself.

Tarski's fixed point theorem

Tarski's Fixed Point theorem shows that in a complete lattice with a monotonic function G on this lattice, there is at least one fixed point of G, namely the least fixed point $\sqcap$Post.

- Tarski's theorem guarantees fixpoints in complete lattices, but the above proof does not say how to find them.
- How difficult it is to find fixpoints depends on the structure of the lattice.

Let G be a monotonic function on a lattice. Let $a_0 = \bot$ and $a_{n+1} = G(a_n)$.
We obtain a sequence $\bot \sqsubseteq G(\bot) \sqsubseteq G^2(\bot) \sqsubseteq \cdots$. Let $a_* = \bigsqcup_{n \geq 0} a_n$.

$/G$

$\bigsqcup_{n \geq 0} a_n \sqsubseteq G(\bigsqcup_{n \geq 0} a_n)$

Lemma: The value a_* is a prefix point.
Observation: a_* need not be a fixpoint (e.g. on lattice [0,1] of real numbers).

$a_* \sqsubseteq G(a_*)$

$\underbrace{a_n}_{G^n(\bot)} \sqsubseteq G(\bigsqcup_{n \geq 0} a_n) \sqsupseteq G^{n+1}(\bot) \; /G$

Omega continuity

Definition: A function G is ω-continuous if for every chain $x_0 \sqsubseteq x_1 \sqsubseteq \ldots \sqsubseteq x_n \sqsubseteq \ldots$ we have

$$G(\bigsqcup_{i \geq 0} x_i) = \bigsqcup_{i \geq 0} G(x_i)$$

Lemma: For an ω-continuous function G, the value $a_* = \bigsqcup_{n \geq 0} G^n(\perp)$ is the least fixpoint of G.

Iterating sequences and omega continuity

Lemma: For an ω-continuous function G, the value $a_* = \bigsqcup_{n\geq 0} G^n(\bot)$ is the least fixpoint of G.

Proof:

- By definition of ω-continuous we have $G(\bigsqcup_{n\geq 0} G^n(\bot)) = \bigsqcup_{n\geq 0} G^{n+1}(\bot) = \bigsqcup_{n\geq 1} G^n(\bot)$.
- But $\bigsqcup_{n\geq 0} G^n(\bot) = \bigsqcup_{n\geq 1} G^n(\bot) \sqcup \bot = \bigsqcup_{n\geq 1} G^n(\bot)$ because $\bot$ is the least element of the lattice.
- Thus $G(\bigsqcup_{n\geq 0} G^n(\bot)) = \bigsqcup_{n\geq 0} G^n(\bot)$ and a_* is a fixpoint. $G(a_*) = a_*$

Now let's prove it is the least. Let c be such that $G(c) = c$. We want $\bigsqcup_{n\geq 0} G^n(\bot) \sqsubseteq c$. This is equivalent to $\forall n \in \mathbb{N}. G^n(\bot) \sqsubseteq c$.
We can prove this by induction : $\bot \sqsubseteq c$ and if $G^n(\bot) \sqsubseteq c$, then by monotonicity of G and by definition of c we have $G^{n+1}(\bot) \sqsubseteq G(c) \sqsubseteq c$.

Iterating sequences and omega continuity

Lemma: For an ω-continuous function G, the value $a_* = \bigsqcup_{n \geq 0} G^n(\perp)$ is the least fixpoint of G.

When the function is not ω-continuous, then we obtain a_* as above (we jump over a discontinuity) and then continue iterating. We then take the limit of such sequence, and the limit of limits etc., ultimately we obtain the fixpoint.

Exercise

Let $C[0,1]$ be the set of continuous functions from $[0,1]$ to the reals. Define $\leq$ on $C[0,1]$ by $f \leq g$ if and only if $f(a) \leq g(a)$ for all $a \in [0,1]$.

i) Show that $\leq$ is a partial order and that $C[0,1]$ with this order forms a lattice.

ii) Does an analogous statement hold if we consider the set of differentiable functions from $[0,1]$ to the reals? That is, instead of requiring the functions to be continuous, we require them to have a derivative on the entire interval. (The order is defined in the same way.)

Exercise

Let $A = [0,1] = \{x \in \mathbb{R} \mid 0 \le x \le 1\}$ be the interval of real numbers. Recall that, by definition of real numbers and complete lattice, $(A, \le)$ is a complete lattice with least lattice element 0 and greatest lattice element 1. Here $\sqcup$ is the least upper bound operator on sets of real numbers, also called *supremum* and denoted *sup* in real analysis.

Let function $f : A \to A$ be given by

$\frac{1}{2} + \frac{1}{4}x = x$

$\frac{1}{2} = \frac{3}{4}x$

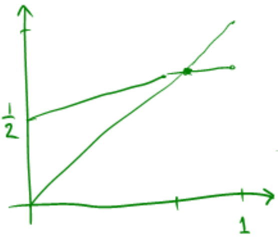
$\frac{1}{2} + \frac{1}{4} \cdot \frac{2}{3} = \frac{1}{2} + \frac{1}{6} = \frac{2}{3}$

$\frac{3}{5} + \frac{1}{5} \cdot \frac{2}{3} = \frac{9+2}{15} = \frac{11}{15}$

$\frac{11}{15}$

$$f(x) = \begin{cases} \frac{1}{2} + \frac{1}{4}x, & \text{if } x \in [0, \frac{2}{3}) \\ \frac{3}{5} + \frac{1}{5}x, & \text{if } x \in [\frac{2}{3}, 1] \end{cases}$$

$\frac{3}{5} + \frac{1}{5}x = x$



(It may help you to try to draw f.)

a) Prove that f is monotonic and injective (so it is strictly monotonic).

b) Compute the set of fixpoints of f.

$f(iter(x)) \neq iter(x) = \frac{2}{3}$

c) Define $iter(x) = \sqcup\{f^n(x) \mid n \in \{0, 1, 2, \ldots\}\}$. (This is in fact equal to $\lim_{n\to\infty} f^n(x)$ when f is a monotonic bounded function.)

Compute $iter(0)$ (prove that the computed value is correct by definition of *iter*, that is, that the value is indeed $\sqcup$ of the set of values). Is $iter(0)$ a fixpoint of f? Is $iter(iter(0))$ a fixpoint of f?