Ordered Sets and Fixpoints

(Based on [Davey and Priestley 2002])

Yih-Kuen Tsay

Dept. of Information Management
National Taiwan University

Partial Orders

- Let P be a set.
- A *partial order*, or simply *order*, on P is a binary relation $\leq$ on P such that:
  1. $\forall x \in P, x \leq x$, (reflexivity)
  2. $\forall x, y, z \in P, x \leq y \wedge y \leq z \rightarrow x \leq z$, (transitivity)
  3. $\forall x, y \in P, x \leq y \wedge y \leq x \rightarrow x = y$. (antisymmetry)
- A set P equipped with a partial order $\leq$, often written as $\langle P, \leq \rangle$, is called a *partially ordered set*, or simply *ordered set*, sometimes abbreviated as *poset*.
- A binary relation that is reflexive and transitive is called a *pre-order* or *quasi-order*.
- We write $x < y$ to mean $x \leq y$ and $x \neq y$.

Examples of Ordered Sets

- $\langle \mathcal{N}, \leq \rangle$
  - $\mathcal{N} = \{1, 2, 3, \cdots\}$, the set of natural numbers.
  - $\leq$ is the usual "less than or equal to" relation.

  Variant: $\langle \mathcal{N}_0, \leq \rangle$ with $\mathcal{N}_0 = \mathcal{N} \cup \{0\} = \{0, 1, 2, 3, \cdots\}$.
- $\langle \mathcal{P}(X), \subseteq \rangle$
  - $\mathcal{P}(X)$ is the powerset of X, consisting of all subsets of X.
  - $\subseteq$ is the set inclusion relation.
- $\langle \Sigma^*, \leq \rangle$
  - Σ^* is the set of all finite strings over the alphabet Σ.
  - $\leq$ is the "is a prefix of" relation.

Order-Isomorphisms

- We want to be able to tell when two ordered sets are essentially the same.
- Let $\langle P, \leq_P \rangle$ and $\langle Q, \leq_Q \rangle$ be two ordered sets.
- P and Q are said to be (*order-*)*isomorphic*, denoted $P \cong Q$, if there is a map φ from P onto Q such that $x \leq_P y$ if and only if $\varphi(x) \leq_Q \varphi(y)$.
- The map φ above is called an *order-isomorphism*.
- For example, $\mathcal{N}_0$ and $\mathcal{N}$ are order-isomorphic with the successor function $n \mapsto n + 1$ as the order-isomorphism.
- An order-isomorphism is necessarily *bijective* (one-to-one and onto). Therefore, an order-isomorphism $\varphi : P \to Q$ has a well-defined inverse $\varphi^{-1} : Q \to P$.

Chains and Antichains

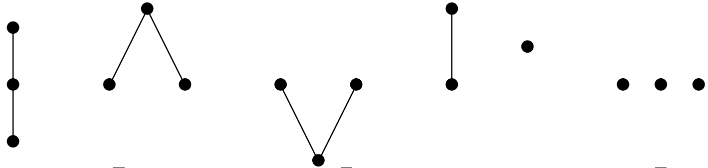
- Let P be an ordered set.
- P is called a *chain* if $\forall x, y \in P, x \leq y \vee y \leq x$, i.e., any two elements in P are comparable.
- For example, $\langle \mathcal{N}, \leq \rangle$ is a chain.
- Alternative names for a chain are *totally ordered set* and *linearly ordered set*.
- P is called an *antichain* if $\forall x, y \in P, x \leq y \to x = y$, i.e., no two distinct elements in P are ordered.
- Clearly, any subset of a chain (an antichain) is a chain (an antichain).
- We write $\mathbf{n}$ to denote a chain of n elements and $\bar{\mathbf{n}}$ an antichain of n elements.

Sums of Ordered Sets

- Let P and Q be two *disjoint* ordered sets.
- The disjoint union $P \uplus Q$ is defined by $x \leq y$ in $P \uplus Q$ if and only if
  1. $x, y \in P$ and $x \leq y$ in P, or
  2. $x, y \in Q$ and $x \leq y$ in Q.
- The linear sum $P \oplus Q$ is defined by $x \leq y$ in $P \oplus Q$ if and only if
  1. $x, y \in P$ and $x \leq y$ in P, or
  2. $x, y \in Q$ and $x \leq y$ in Q, or
  3. $x \in P$ and $y \in Q$.

Diagrams for Ordered Sets

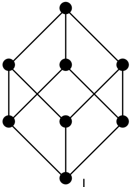
- All possible ordered sets with three elements:



$\mathbf{3}$ $\quad \bar{\mathbf{2}} \oplus \mathbf{1}$ $\quad \mathbf{1} \oplus \bar{\mathbf{2}}$ $\quad \mathbf{2} \uplus \mathbf{1}$ $\quad \bar{\mathbf{3}}$

- $\langle \mathcal{P}(\{1,2,3\}), \subseteq \rangle$:

$\top = \{1,2,3\}$



$\bot = \emptyset$

Partial Maps

- A (total) map or function f from X to Y is a binary relation on X and Y satisfying the following conditions:
  1. (single-valued) For every $x \in X$, there is at most one $y \in Y$ such that (x, y) is related by f.
     In other words, if both (x, y_1) and (x, y_2) are related by f, then y_1 and y_2 must be equal.
  2. (total) For every $x \in X$, there is at least one $y \in Y$ such that (x, y) is related by f.
- A *partial map* f from X to Y is a *single-valued*, not necessarily total, binary relation on X and Y.
- Representation of a total or partial map f from X to Y as a subset of $X \times Y$, or as an element of $\mathcal{P}(X \times Y)$, is called the *graph* of f, denoted $\mathrm{graph}(f)$.

Partial Maps as an Ordered Set

- We write $(X \rightarrowtriangle Y)$ to denote the set of all partial maps from X to Y.
- For $\sigma, \tau \in (X \rightarrowtriangle Y)$, we define $\sigma \leq \tau$ if and only if $\mathrm{graph}(\sigma) \subseteq \mathrm{graph}(\tau)$.
  In other words, $\sigma \leq \tau$ if and only if whenever $\sigma(x)$ is defined, $\tau(x)$ is also defined and equals $\sigma(x)$.
- $\langle (X \rightarrowtriangle Y), \leq \rangle$ is an ordered set.

Programs as Partial Maps

- Two programs P and Q with common sets X and Y respectively of *initial* states and *final* states may be seen as defining two partial maps $\sigma_P, \sigma_Q : X \rightarrowtriangle Y$.
- The two programs might be related by $\sigma_P \leq \sigma_Q$, meaning that
  - for any input state from which P terminates, Q also terminates, and
  - for every case where P terminates, Q produces the same output as P does.
- When $\sigma_P \leq \sigma_Q$ does hold, we say P is refined by Q or Q refines P. (Some prefer the opposite.)
- The refinement relation between two programs as defined is clearly a partial order.

Order-Preserving Maps

- Let P and Q be ordered sets.
- A map $\varphi : P \rightarrow Q$ is said to be order-preserving (or monotone) if $x \leq y$ in P implies $\varphi(x) \leq \varphi(y)$ in Q.
- The composition of two order-preserving maps is also order-preserving.
- A map $\varphi : P \rightarrow Q$ is said to be an order-embedding (denoted $P \hookrightarrow Q$) if $x \leq y$ in P if and only if $\varphi(x) \leq \varphi(y)$ in Q.

Galois Connections and Insertions

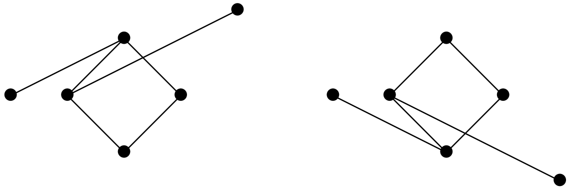
- Let P and Q be ordered sets.
- A pair (α, γ) of maps $\alpha : P \to Q$ and $\gamma : Q \to P$ is a *Galois connection* between P and Q if, for all $p \in P$ and $q \in Q$,

$$\alpha(p) \leq q \leftrightarrow p \leq \gamma(q)$$

- Alternatively, (α, γ) is a Galois connection between P and Q if, for all $p, p_1, p_2 \in P$, $q, q_1, q_2 \in Q$,
  1. $p_1 \leq p_2 \to \alpha(p_1) \leq \alpha(p_2)$ and $q_1 \leq q_2 \to \gamma(q_1) \leq \gamma(q_2)$ (i.e., α and γ are monotone)
  2. $p \leq \gamma(\alpha(p))$ and $\alpha(\gamma(q)) \leq q$.
- A *Galois insertion* is a Galois connection where $\alpha \circ \gamma$ is the identity map, i.e., $\alpha(\gamma(q)) = q$.

Dual of an Ordered Set

- Given an ordered set P, we can form a new ordered set P^∂ (the "dual of P") by defining $x \leq y$ to hold in P^∂ if and only if $y \leq x$ holds in P.
- For a finite P, a diagram for P^∂ can be obtained by turning upside down a diagram for P:



P $\qquad$ P^∂

The Duality Principle

- For a statement Φ about ordered sets, its dual statement Φ^∂ is obtained by replacing each occurrence of $\leq$ with $\geq$ and vice versa.
- The Duality Principle: Given a statement Φ about ordered sets that is true for all ordered sets, the dual statement Φ^∂ is also true for all ordered sets.

Bottom and Top

- Let P be an ordered set.
- P has a bottom element if there exists $\bot \in P$ ("bottom") such that $\bot \leq x$ for all $x \in P$.
- Dually, P has a top element if there exists $\top \in P$ ("top") such that $x \leq \top$ for all $x \in P$.
- $\bot$ is unique when it exists; dually, $\top$ is unique when it exists.
- In $\langle \mathcal{P}(X), \subseteq \rangle$, we have $\bot = \emptyset$ and $\top = X$.
- A finite chain always has a bottom and a top elements; this may not hold for an infinite chain.
- Given a bottomless P, we may form $P_\bot$ (P lifted or the lifting of P) by $P_\bot \triangleq \mathbf{1} \oplus P$.

Maximal and Minimal Elements

- Let P be an ordered set and $S \subseteq P$.
- An element $a \in S$ is a *maximal element* of S if $a \leq x$ and $x \in S$ imply $x = a$.
- If Q has a top element $\top_Q$, it is called the *greatest element* (or *maximum*) of Q.
- A *minimal element* of S and the *least element* (or *minimum*) of S (if it exists) are defined dually.

Down-sets and Up-sets

- Let P be an ordered set and $S \subseteq P$.
- S is a *down-set* (order ideal) if, whenever $x \in S$, $y \in P$, and $y \leq x$, we have $y \in S$.
- Dually, S is a *up-set* (order filter) if, whenever $x \in S$, $y \in P$, and $y \geq x$, we have $y \in S$.
- Given an arbitrary $Q \subseteq P$ and $x \in P$, we define
  - $\downarrow Q \triangleq \{y \in P \mid \exists x \in Q, y \leq x\}$ ("down Q"),
  - $\uparrow Q \triangleq \{y \in P \mid \exists x \in Q, y \geq x\}$ ("up Q"),
  - $\downarrow x \triangleq \{y \in P \mid y \leq x\}$, and
  - $\uparrow x \triangleq \{y \in P \mid y \geq x\}$.
- $\downarrow Q$ is the smallest down-set containing Q and Q is a down-set if and only if $Q = \downarrow Q$; dually for $\uparrow Q$.

Upper and Lower Bounds

IM NTU

- Let P be an ordered set and $S \subseteq P$.
- An element $x \in P$ is an *upper bound* of S if, for all $s \in S$, $s \leq x$.
- Dually, an element $x \in P$ is an *lower bound* of S if, for all $s \in S$, $s \geq x$ (or $x \leq s$).
- The set of all upper bounds of S is denoted by S^u ("S upper"); $S^u = \{x \in P \mid \forall s \in S, s \leq x\}$.
- The set of all lower bounds of S is denoted by S^l ("S lower"); $S^l = \{x \in P \mid \forall s \in S, s \geq x\}$.
- By convention, $\emptyset^u = P$ and $\emptyset^l = P$.
- Since $\leq$ is transitive, S^u is an up-set and S^l a down-set.

Least Upper and Greatest Lower Bounds

IM NTU

- Let P be an ordered set and $S \subseteq P$.
- If S^u has a least element, it is called the *least upper bound* (supremum) of S, denoted $\sup(S)$.
- Equivalently, x is the least upper bound of S if
  - x is an upper bound of S, and
  - for every upper bound y of S, $x \leq y$.
- Dually, if S^l has a greatest element, it is called the *greatest lower bound* (infimum) of S, denoted $\inf(S)$.
- When P has a top element, $P^u = \{\top\}$ and $\sup(P) = \top$. Dually, if P has a bottom element, $P^l = \{\bot\}$ and $\inf(P) = \bot$.
- Since $\emptyset^u = \emptyset^l = P$, $\sup(\emptyset)$ exists if P has a bottom element; dually, $\inf(\emptyset)$ exists if P has a top element.

Join and Meet

- We write $x \vee y$ ("x join y") in place of $\sup(\{x, y\})$ when it exists and $x \wedge y$ ("x meet y") in place of $\inf(\{x, y\})$ when it exists.
- Let P be an ordered set. If $x, y \in P$ and $x \leq y$, $x \vee y = y$ and $x \wedge y = x$.
- In the following two cases, $a \vee b$ does not exist.

- Analogously, we write $\bigvee S$ (the "join of S") and $\bigwedge S$ (the "meet of S").

Lattices and Complete Lattices

- Let P be a *non-empty* ordered set.
- P is called a *lattice* if $x \vee y$ and $x \wedge y$ exist for all $x, y \in P$.
- P is called a *complete lattice* if $\bigvee S$ and $\bigwedge S$ exist for all $S \subseteq P$.
  Note: as S may be empty, the definition implies that every complete lattice is *bounded*, i.e., it has *top* and *bottom* elements.
- Every finite lattice is complete.

Fixpoints

- Given an ordered set P and a map $F : P \to P$, an element $x \in P$ is called a *fixpoint* of F if $F(x) = x$.
- The set of fixpoints of F is denoted $\mathrm{fix}(F)$.
- The least element of $\mathrm{fix}(F)$, when it exists, is denoted $\mu(F)$, and the greatest by $\nu(F)$ if it exists.

A Fixpoint Theorem for Complete Lattices

IM NTU

Theorem (Knaster-Tarski Fixpoint Theorem)

Let L be a complete lattice and $F : L \to L$ an order-preserving map. Then,

$$\mu(F) = \bigwedge\{x \in L \mid F(x) \leq x\}.$$

Dually, $\nu(F) = \bigvee\{x \in L \mid x \leq F(x)\}$.

- Let $M = \{x \in L \mid F(x) \leq x\}$ and $\alpha = \bigwedge M$. We need to show (1) $F(\alpha) = \alpha$ and (2) for every $\beta \in \mathrm{fix}(F)$, $\alpha \leq \beta$.
- For all $x \in M$, $\alpha \leq x$ and so $F(\alpha) \leq F(x) \leq x$. Thus, $F(\alpha) \in M^l$ and hence $F(\alpha) \leq \alpha$ $(= \bigwedge M)$.
- $F(F(\alpha)) \leq F(\alpha)$, implying $F(\alpha) \in M$ and so $\alpha \leq F(\alpha)$.
- For every $\beta \in \mathrm{fix}(F)$, $\beta \in M$ and hence $\alpha \leq \beta$.

Chain Conditions

- Let P be an ordered set.
- P satisfies the ascending chain condition (ACC), if given any sequence $x_1 \leq x_2 \leq \cdots \leq x_n \leq \cdots$ of elements in P, there exists $k \in N$ such that $x_k = x_{k+1} = \cdots$.
- Dually, P satisfies the descending chain condition (DCC), if given any sequence $x_1 \geq x_2 \geq \cdots \geq x_n \geq \cdots$ of elements in P, there exists $k \in N$ such that $x_k = x_{k+1} = \cdots$.

Directed Sets

- Let S be a *non-empty* subset of an ordered set.
- S is said to be *directed* if, for every pair of elements $x, y \in S$ there exists $z \in S$ such that $z \in \{x, y\}^u$.
- S is directed if and only if, for every finite subset F of S, there exists $z \in S$ such that $z \in F^u$.
- In an ordered set with the ACC, a set is directed if and only if it has a greatest element.
- When D is directed for which $\bigvee D$ exists, we write $\bigsqcup D$ in place of $\bigvee D$.

Complete Partial Orders (CPO)

- An ordered set P is called a *Complete Partial Order* (*CPO*) if
  1. P has a bottom element $\perp$ and
  2. $\bigsqcup D$ exists for each directed subset D of P.
- Alternatively, P is a CPO if each chain of P has a least upper bound in P.
- Any complete lattice is a CPO.
- For an ordered P satisfying Condition 2 above (called a pre-CPO), its lifting $P_\perp$ is a CPO.

Continuous Maps

- Let P and Q be CPOs.
- A map $\varphi : P \to Q$ is said to be continuous if, for every directed set D in P,
  1. the subset $\varphi(D)$ of Q is directed and
  2. $\varphi(\bigsqcup D) = \bigsqcup \varphi(D)$.
- A continuous map need not preserve bottoms, since by definition the empty set is not directed.
- A map $\varphi : P \to Q$ such that $\varphi(\bot) = \bot$ is called strict.

A Fixpoint Theorem for CPOs

- The n-fold composite F^n of $F : P \to P$ is defined as follows.
  1. F^0 is the identity.
  2. $F^n = F \circ F^{n-1}$ for $n \geq 1$.
- If F is order-preserving, so is F^n.

Theorem (CPO Fixpoint Theorem I)

Let P be a CPO and $F : P \to P$ an order-preserving map. Define $\alpha \triangleq \bigsqcup_{n \geq 0} F^n(\bot)$.

1. *If $\alpha \in \mathrm{fix}(F)$, then $\alpha = \mu(F)$.*
2. *If F is continuous, then $\mu(F)$ exists and equals α.*

Proof of CPO Fixpoint Theorem I (1)

- $\perp \leq F(\perp)$. So, $F^n(\perp) \leq F^{n+1}(\perp)$, for all n, inducing a chain in P:

$$\perp \leq F(\perp) \leq F^2(\perp) \leq \cdots \leq F^n(\perp) \leq F^{n+1}(\perp) \leq \cdots$$

- Since P is a CPO, $\alpha \triangleq \bigsqcup_{n \geq 0} F^n(\perp)$ exists.
- Let β be any fixpoint of F; we need to show that $\alpha \leq \beta$.
- By induction, $F^n(\beta) = \beta$, for all n.
- We have $\perp \leq \beta$, hence $F^n(\perp) \leq F^n(\beta) = \beta$.
- The definition of α then ensures $\alpha \leq \beta$.

Proof of CPO Fixpoint Theorem I (2)

- It suffices to show that $\alpha \in \mathrm{fix}(F)$.
- We have

$$
\begin{array}{rcll}
F(\bigsqcup_{n \geq 0} F^n(\bot)) & = & \bigsqcup_{n \geq 0} F(F^n(\bot)) & (F \text{ continuous}) \\
 & = & \bigsqcup_{n \geq 1} F^n(\bot) & \\
 & = & \bigsqcup_{n \geq 0} F^n(\bot) & (\bot \leq F^n(\bot) \text{ for all } n)
\end{array}
$$

Another Fixpoint Theorem for CPOs

IM NTU

Theorem (CPO Fixpoint Theorem II)

Let P be a CPO and $F : P \to P$ an order-preserving map. Then F has a least fixpoint.