Algebraic and Coalgebraic Methods in the Mathematics of Program Construction

Definitions and main results

1 Chapter 2

- Main reference is B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order*. Cambridge Mathematical Textbooks. Cambridge University Press
- Conventions
  - Dual posets are identified by a ∂ superscript: $P \longrightarrow P^\partial$
  - Powersets are identified using the symbol $\wp$, as in the powerset of set G is $\wp(G)$
  - Set difference uses $\setminus$ as in $A \setminus B$ being A minus B
  - Bottom element is $\perp$, top element is $\top$
- Context

  Given sets G and M and a binary relation $R \subseteq G \times M$ a **context** is the triple (G, M, R)
- Polars

  Given the context (G, M, R) the **polars** of A and B are the elements of the other set that are related to **all** elements in the given set

  $$A^{\triangleright} \equiv \{m \in M : (\forall g \in A)(g, m) \in R\}, \qquad \text{for } A \subseteq G$$
  $$B^{\triangleleft} \equiv \{g \in G : (\forall m \in B)(g, m) \in R\}, \qquad \text{for } B \subseteq M$$

  Polars are monotone when taken as $\triangleleft : \wp(G) \to \wp(M)^\partial$ and $\triangleright : \wp(M)^\partial \to \wp(G)$. Polars establish a Galois connection between the powersets.
- Concepts

  Given $A \subseteq G$ and $B \subseteq M$ we call (A, B) a **concept** if $A = B^{\triangleleft}$ and $A^{\triangleright} = B$. Concepts are ordered by inclusion on the first co-ordinate and reverse inclusion on the second, which is the order of $\wp(G) \times \wp(M)^\partial$.

  The set of all ordered concepts is denoted $\mathfrak{B}(G, M, R)$.

- A **chain** is a poset in which any two elements are comparable; its order is a **linear** or **total** order. An **antichain** is a poset where $\leqslant$ coincides with $=$
- Bottom: $\forall x \in P : \perp \leqslant x$. Top: $\forall x \in P : x \leqslant \top$.
- A finite chain always has $\top$ and $\perp$
- Lifting

  Given any poset P we form $P_\perp$ called P lifted by adding a new element $\perp \notin P$ and defining

  $$x \leqslant_{P_\perp} y \iff x = \perp \text{ or } x \leqslant y \text{ in } P$$

- Sums and products, defined for disjoint posets
  - **Linear Sum** $P \oplus Q$ is the poset Q "on top" of P. The elements are the union of the elements of both, with their respective order and $x \leqslant y$ if $x \in P$ and $y \in Q$
  - **Union** or **Disjoint Union** $P \dot\cup Q$. The elements are the union of the elements of both, with the order defined only between elements of the same poset
  - **Product** $P \times Q$, the elements are the ordered pairs $\{(p,q) : p \in P, q \in Q\}$, ordered according to the order in *both* components.
- Maps between posets
  - **Monotone** or **order-preserving**: $x \leqslant_P y \implies F(x) \leqslant_Q F(y)$
  - **Order-embedding**: $x \leqslant_P y \iff F(x) \leqslant_Q F(y)$. An order embedding is always injective (one-to-one)
  - **Order-isomorphism**: order embedding *onto* Q. A monotone map is an isomorphism iff there is a monotone inverse.
- A **predicate** is a function from X to $\{\mathbf{T}, \mathbf{F}\}$. The poset of predicates on X $\mathbb{P}(X)$ is ordered by

  $$p \Rrightarrow q \text{ if and only if } \{x \in X : p(x) = \mathbf{T}\} \subseteq \{x \in X : q(x) = \mathbf{T}\}$$

  There is an isomorphism $F : \langle \mathbb{P}(X); \Rrightarrow \rangle \to \langle \wp(X); \subseteq \rangle$ given by $F(p) \equiv \{x \in X : p(x) = \mathbf{T}\}$

- Pointwise ordering. Given any set X and a poset P we can define an order for maps $F, G : X \to Q$ (notated as Q^X) as

  $$F \sqsubseteq G \iff (\forall x \in X)\, F(x) \leqslant G(x)$$

  If X is also a poset we write the poset of maps as $\langle P \to Q \rangle$

- $\uparrow x \equiv \{y \in P : y \geqslant x\}$. The set of all elements $\geqslant x$

- Up-sets. $Y \subseteq P$ is an **up-set** of P if $x \in P, x \geqslant y, y \in Y$ implies $x \in y$. So, if Y is closed above: it includes all the elements larger than any of the members.
- The family of all up-sets ordered by inclusion is a poset denoted by $\mathcal{U}(P)$. If $A_i \in \mathcal{U}(P)$ then $\bigcup_{i \in I} A_i$ and $\bigcap_{i \in I} A_i$ also belong to $\mathcal{U}(P)$
- Dually to up-sets we define $\downarrow x$ and $\mathcal{O}(P)$ as the family of all down-sets of P
- A **tree** is a poset with bottom such that $\downarrow x$ is a chain for all $x \in P$
- $Y \in \mathcal{O}(P) \iff P \setminus Y \in \mathcal{U}(P)$
- $\mathcal{O}(P) \cong \mathcal{U}(P)^\partial$
- $\mathcal{U}(P)^\partial \cong \mathcal{U}(P^\partial)$ and $\mathcal{O}(P)^\partial \cong \mathcal{O}(P^\partial)$
- The following are equivalent:

$$
\begin{gathered}
x \leqslant y \\
\downarrow x \subseteq \downarrow y \\
(\forall Y \in \mathcal{O}(P)) \quad y \in Y \implies x \in Y
\end{gathered}
$$

- The up arrow can also be defined for subsets: $\downarrow Y \equiv \bigcup \{\downarrow y : y \in Y\}$. $\downarrow Y = \downarrow\downarrow Y$. $\downarrow Y = Y \iff Y \in \mathcal{O}(P)$
- $A^\rhd = P \setminus \downarrow A$, $B^\lhd = P \setminus \uparrow B$
- $(A, B) \in \wp(P) \times \wp(P)^\partial$ is a concept iff $A \in \mathcal{O}(P)$ and $B \in \mathcal{U}(P)$ with $A = P \setminus B$
- A **maximal** element of a subset S is such that there are no larger elements in S: m is maximal if $a \leqslant x \in S \implies a = x$. The set of maximal elements of the subset is denoted by $\operatorname{Max} S$
- A non-empty poset L is a lattice if for $x, y \in L$ there exists elements $x \vee y$ and $x \wedge y$ in L such that

$$
\uparrow x \cap \uparrow y = \uparrow (x \vee y) \quad \text{and} \quad \downarrow x \cap \downarrow y = \downarrow (x \wedge y)
$$

- **Connecting lemma**: $x \wedge y = x \iff x \leqslant y \iff x \vee y = y$
- Finite lattices posses top and bottom
- It can be shown that $\vee$ and $\wedge$ are associative, commutative, idempotent and that $x \vee (x \wedge y) = x$. I had to use the fact that $\uparrow$ and $\downarrow$ are injective, which seems to be an important result not stated explicitly in the book
- $a \leqslant b \implies a \vee c \leqslant b \vee c$ and $a \wedge c \leqslant b \wedge c$
- $a \leqslant b$ and $c \leqslant d \implies a \vee c \leqslant b \vee d$ and $a \wedge c \leqslant b \wedge d$

- $\mathfrak{L} \subseteq \wp(X)$ is a **lattice of sets** if it is closed under *finite* unions and intersections. $A \vee B = A \cup B; A \wedge B = A \cap B$. $\mathcal{U}(P)$ and $\mathcal{O}(P)$ are lattices of sets.

- A **distribute lattice** has the properties

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

- A **boolean algebra** is a distributive lattice possessing bottom, top and a unary operation of complement $'$ such that $x \vee x' = \top$ and $x \wedge x' = \bot$

- The sets of **upper bounds** and **lower bounds** are defined for any $S \subseteq P$ as the elements of P that are larger/smaller than all the elements in S. Notice that in general $S^u \nsubseteq S$

$$S^u \equiv \{x \in P : (\forall s \in S)\ x \geqslant s\} = \bigcap \{\uparrow s : s \in S\}$$
$$S^\ell \equiv \{x \in P : (\forall s \in S)\ x \leqslant s\} = \bigcap \{\downarrow s : s \in S\}$$

- For any subset S of a poset P the **supremum** or **least upper bound** or **join** α of S exists if

$$(\forall s \in S)\ s \leqslant \alpha \qquad \alpha \text{ is an upper bound}$$
$$(\forall x \in S^u)\ \alpha \leqslant x \qquad \alpha \text{ is the least upper bound}$$

- $\sup \emptyset = \bot; \inf \emptyset = \top$

- A **complete lattice** is a non-empty poset for which $\bigwedge S$ and $\bigvee S$ exist for all (potentially infinite) $S \subseteq P$ including $S = \emptyset$. So, a complete lattice has top and bottom.

- If P has top and $\bigwedge S$ exists for every non-empty subset, then P is a lattice

- Any finite lattice is complete

- A poset satisfies the **ascending chain condition (ACC)** if it has no infinite ascending sequences $x_1 \leqslant x_2 \leqslant \ldots$

- A poset satisfies ACC iff $\operatorname{Max} S \neq \emptyset$ for $\emptyset \neq S \subseteq P$

- A lattice that satisfies ACC and has bottom is complete

- Any map between lattices preserving $\vee$ or $\wedge$ is monotone

- Order isomorphisms preserve all existing sups and infs

- A **complete lattice of sets** is a non-empty family $\mathcal{L}$ of subsets of X that is closed under (possibly infinite) unions and intersections

- Every poset has an associated topology with the up-sets as the open sets

- A **closure system** $\mathcal{L}$ (aka. topped intersection structure) is a non-empty family of subsets of X which satisfies:

$$\bigwedge_{i \in I} A_i \in \mathcal{L} \text{ for every non-empty family } \{A_i\}_{i \in I} \subseteq \mathcal{L} \tag{cs1}$$

$$X \in \mathcal{L} \tag{cs2}$$

  If $\mathcal{L}$ satisfies only (cs1), then it is an **intersection structure**.

- A closure system is a complete lattice with

$$\bigwedge_{i \in I} = \bigcap_{i \in I} A_i$$
$$\bigvee_{i \in I} = \bigcap \left\{ B \in \mathcal{L} : \bigcup_{i \in I} A_i \subseteq B \right\}$$

- Every complete lattice L is isomorphic to a closure system $\mathcal{L} = \{\downarrow x : x \in L\}$

- A map $c : P \to P$ is a **closure operator**[1] if $\forall x, y \in P$

$$x \leqslant c(x)$$
$$x \leqslant y \implies c(x) \leqslant c(y)$$
$$c(c(x)) = c(x)$$

- $x \in P$ is a **closed** element if $c(x) = x$. The set of all closed elements is P_c

- $\uparrow$ and $\downarrow$ are closed operators with up-sets and and down-sets as closed sets.

- Prefix lemma: if $c : P \to P$ is monotone, $Q = \{x \in P : c(x) \leqslant x\}$ is a complete lattice

- For a closure operator c

$$c(P) = P_c = \{x \in P : c(x) = x\}$$

  ($c(P)$ is the image of P under c) is a complete lattice with

$$\bigwedge_{P_c} S = \bigwedge_P S \qquad \bigvee_{P_c} S = c\left(\bigvee_P S\right) \qquad \top_{c(P)} = c(\top_P)$$

- $C_{\mathcal{L}_C} = C$ and $\mathcal{L}_{C_\mathcal{L}} = \mathcal{L}$

- Given maps (initially not necessarily monotone) $F : P \to Q$ and $G : Q \to P$, (F, G) is a **Galois connection**[2] iff

$$F(p) \leqslant q \iff p \leqslant G(q) \quad \text{for all } p \in P, q \in Q$$

[1] Note this is nothing more than a monad

[2] This is just an adjunction between the posets seen as categories. But notice the maps are not required to be monotone (functors), monotonicity is going to be a consequence of the adjunction.

- We write the left (lower) adjoint as $\rhd$ and the right (upper) one as $\lhd$
- Polars under a relation form a Galois connection: $\rhd$: $\wp(G) \to \wp(M)^\partial$ and $\lhd$: $\wp(M)^\partial \to \wp(G)$
- Upper and lower bounds are form a Galois connection: $(^u, ^\ell)$ between $\wp(P) \to \wp(P)^\partial$
- An important theorem: if $(^\rhd, ^\lhd)$ is a Galois connection between P and Q:

Cancellation rule:	$p \leqslant p^{\rhd\lhd}$ and $q^{\lhd\rhd} \leqslant q$	(Gal1)
Monotonicity rule:	$^\rhd, ^\lhd$ are monotone	(Gal2)
Semi-inverse rule:	$p^{\rhd\lhd\rhd} = p^\rhd$ and $q^{\lhd\rhd\lhd} = q^\lhd$	(Gal3)

- $\rhd$ and $\lhd$ have order-isomorphic images
- Equivalent definitions of Galois connection:
  1. $(^\rhd, ^\lhd)$ is a Galois connection
  2. $^\rhd$ and $^\lhd$ are monotone with $p \leqslant p^{\rhd\lhd}$ and $q^{\lhd\rhd} \leqslant q$
  3. $^\rhd$ and $^\lhd$ satisfy:
     (a) $^\rhd$ is monotone
     (b) $q^{\lhd\rhd} \leqslant q$
     (c) $p^\rhd \leqslant q \implies p \leqslant q^\lhd$
- Left adjoints preserve sups, right adjoints preserve infs
- Given a left adjoint the right adjoint is unique and determined (and dual)

$$p^\rhd = \min \{q \in Q : p \leqslant q^\lhd\}$$
$$q^\lhd = \max \{p \in P : p^\rhd \leqslant q\}$$

- Given maps $F : P \to Q$, $G : Q \to P$:
  - If P is a complete lattice then F has an upper adjoint iff F preserves arbitrary sups
  - If Q is a complete lattice then G has a lower adjoint iff G preserves arbitrary infs