

Galois Connections

Roland Backhouse
3rd December, 2002

Fusion

Many problems are expressed in the form

evaluate ◦ *generate*

where *generate* generates a (possibly infinite) candidate set of solutions, and *evaluate* selects a best solution.

Examples:

shortest ◦ *path* ,

$(x \in) \circ L$.

Solution method is to *fuse* the generation and evaluation processes, eliminating the need to generate all candidate solutions.

Conditions for Fusion

Fusion is made possible when

- *evaluate* is an adjoint in a *Galois connection*,
- *generate* is expressed as a *fixed point*.

Solution method typically involves *generalising* the problem.

Definition

Suppose $\mathcal{A} = (A, \sqsubseteq)$ and $\mathcal{B} = (B, \preceq)$ are partially ordered sets and suppose $F \in A \leftarrow B$ and $G \in B \leftarrow A$. Then (F, G) is a *Galois connection of \mathcal{A} and \mathcal{B}* iff, for all $x \in B$ and $y \in A$,

$$F.x \sqsubseteq y \equiv x \preceq G.y .$$

F is called the *lower* adjoint. G is the *upper* adjoint.

Examples — Propositional Calculus

$$\neg p \Rightarrow q \equiv p \Leftarrow \neg q$$

$$p \wedge q \Rightarrow r \equiv q \Rightarrow (p \Rightarrow r)$$

$$p \vee q \Rightarrow r \equiv (p \Rightarrow r) \wedge (q \Rightarrow r)$$

$$p \Rightarrow q \vee r \equiv p \wedge \neg q \Rightarrow r$$

Examples — Set Theory

$$\neg S \subseteq T \equiv S \supseteq \neg T$$

$$S \cap T \subseteq U \equiv T \subseteq \neg S \cup U$$

$$S \cup T \subseteq U \equiv S \subseteq U \wedge T \subseteq U$$

$$S \subseteq T \cup U \equiv S \cap \neg T \subseteq U$$

Examples — Number Theory

$$-x \leq y \equiv x \geq -y$$

$$x+y \leq z \equiv y \leq z-x$$

$$\lceil x \rceil \leq n \equiv x \leq n$$

$$x \uparrow y \leq z \equiv x \leq z \wedge y \leq z$$

$$x \times y \leq z \equiv x \leq z/y \quad \text{for all } y > 0$$

Examples — predicates

$$\text{even.m} \Leftarrow b \equiv (\text{if } b \text{ then } 2 \text{ else } 1) \setminus m$$

$$\text{odd.m} \Rightarrow b \equiv (\text{if } b \text{ then } 1 \text{ else } 2) \setminus m$$

$$x \in S \Leftarrow b \equiv S \supseteq \text{if } b \text{ then } \{x\} \text{ else } \phi$$

$$x \in S \Rightarrow b \equiv S \subseteq \text{if } b \text{ then } U \text{ else } U \setminus \{x\}$$

$$S = \phi \Leftarrow b \equiv S \subseteq \text{if } b \text{ then } \phi \text{ else } U$$

$$S \neq \phi \Rightarrow b \equiv S \subseteq \text{if } b \text{ then } U \text{ else } \phi$$

Examples — programming algebra

Languages (“factors”)

$$L \cdot M \subseteq N \quad \equiv \quad L \subseteq N/M$$

$$L \cdot M \subseteq N \quad \equiv \quad M \subseteq L \setminus N$$

Relations (“residuals”, “weakest pre and post specifications”)

$$R \circ S \subseteq T \quad \equiv \quad R \subseteq T/S$$

$$R \circ S \subseteq T \quad \equiv \quad S \subseteq R \setminus T$$

Examples — program construction

Conditional correctness:

$$\{p\}S\{q\}$$

means that after successful execution of statement S beginning in a state satisfying the predicate p the resulting state will satisfy predicate q .

Weakest liberal precondition

$$\{p\}S\{q\} \equiv p \Rightarrow wlp(S, q)$$

Strongest liberal postcondition

$$\{p\}S\{q\} \equiv slp(S, p) \Rightarrow q$$

Hence

$$slp(S, p) \Rightarrow q \equiv p \Rightarrow wlp(S, q)$$

Alternative Definitions — Cancellation

(F, G) is a Galois connection between the posets (A, \sqsubseteq) and (B, \preceq) iff the following two conditions hold.

(a) For all $x \in B$ and $y \in A$,

$$x \preceq G.(F.x) \quad \text{and} \quad F.(G.y) \leq y \quad .$$

(b) F and G are both monotonic.

Alternative Definitions — Universal Property

(F, G) is a Galois connection between the posets (A, \sqsubseteq) and (B, \preceq) iff the following conditions hold.

- (a) G is monotonic.
- (b) For all $x \in B$, $x \preceq G.(F.x)$.
- (c) For all $x \in B$ and $y \in A$, $x \preceq G.y \Rightarrow F.x \sqsubseteq y$.

Informally, $F.x$ is the least y such that $x \preceq G.y$.

Suprema and Infima

Greatest divisor

$$k \setminus m \wedge k \setminus n \equiv k \setminus \gcd(m, n) \text{ ,}$$

and least common multiple

$$m \setminus k \wedge n \setminus k \equiv \text{lcm}(m, n) \setminus k \text{ .}$$

Definition of Infimum

Suppose $(\mathcal{A}, \sqsubseteq)$ and (\mathcal{B}, \preceq) are partially ordered sets and $f \in \mathcal{A} \leftarrow \mathcal{B}$ is a monotonic function. Then an *infimum* of f is a solution of the equation:

$$x :: \langle \forall a :: a \sqsubseteq x \equiv \langle \forall b :: a \sqsubseteq f.b \rangle \rangle . \quad (1)$$

Equation (1) need not have a solution. If it does, for a given f , we denote its solution by $\sqcap f$. By definition, then,

$$\langle \forall a :: a \sqsubseteq \sqcap f \equiv \langle \forall b :: a \sqsubseteq f.b \rangle \rangle .$$

A *complete* lattice is a partially ordered set in which all functions have an infimum.

Galois connection

$$\langle \forall a :: a \sqsubseteq \sqcap f \equiv \langle \forall b :: a \sqsubseteq f.b \rangle \rangle .$$

$$\langle \forall b :: a \sqsubseteq f.b \rangle$$

$$\equiv \left\{ \begin{array}{l} \bullet \text{ define the function } K \in (\mathcal{A} \leftarrow \mathcal{B}) \leftarrow \mathcal{A} \text{ by } (K.a).b = a \end{array} \right\}$$

$$\langle \forall b :: (K.a).b \sqsubseteq f.b \rangle$$

$$\equiv \left\{ \begin{array}{l} \text{definition of } \dot{\sqsubseteq} \text{ (pointwise ordering on functions)} \end{array} \right\}$$

$$K.a \dot{\sqsubseteq} f .$$

$$a \sqsubseteq \sqcap f \equiv K.a \dot{\sqsubseteq} f .$$

Definition of Supremum

A *supremum* of f is a solution of the equation:

$$x :: \langle \forall a :: x \sqsubseteq a \equiv \langle \forall b :: f.b \sqsubseteq a \rangle \rangle . \quad (2)$$

As for infima, equation (2) need not have a solution. If it does, for a given f , we denote its solution by $\sqcup f$. By definition, then,

$$\langle \forall a :: \sqcup f \sqsubseteq a \equiv \langle \forall b :: f.b \sqsubseteq a \rangle \rangle . \quad (3)$$

A *cocomplete* lattice is a partially ordered set in which all functions have an supremum.

Note: Cocomplete equals complete.

Infimum Preservation

Suppose \mathcal{A} , \mathcal{B} and \mathcal{C} are complete lattices.

Function $f \in \mathcal{A} \leftarrow \mathcal{B}$ is *inf-preserving* if, for all functions $g \in \mathcal{B} \leftarrow \mathcal{C}$,

$$f.(\sqcap g) = \sqcap(f \bullet g) \ .$$

Suppose that \mathcal{B} is a poset and \mathcal{A} is a complete poset. Then a monotonic function $G \in \mathcal{B} \leftarrow \mathcal{A}$ is an upper adjoint in a Galois connection equivalent to G is inf-preserving.

Dually, a monotonic function $F \in \mathcal{A} \leftarrow \mathcal{B}$ is a lower adjoint in a Galois connection equivalent to F is sup-preserving.

Examples

$$(p \wedge q \Rightarrow r) \equiv (p \Rightarrow (q \Rightarrow r))$$

Hence,

$$p \wedge \langle \exists x :: q.x \rangle \equiv \langle \exists x :: p \wedge q.x \rangle .$$

$$(\neg p \Rightarrow q) \equiv (p \Leftarrow \neg q)$$

Hence,

$$\neg \langle \forall x :: p.x \rangle \equiv \langle \exists x :: \neg(p.x) \rangle$$

$$x \in S \Rightarrow b \equiv S \subseteq \text{if } b \text{ then } U \text{ else } U \setminus \{x\}$$

Hence,

$$x \in \cup S \equiv \langle \exists P : P \in S : x \in P \rangle$$

$$x \in S \Leftarrow b \equiv S \supseteq \text{if } b \text{ then } \{x\} \text{ else } \phi$$

Hence,

$$x \in \cap S \equiv \langle \forall P : P \in S : x \in P \rangle$$