Galois Connections

Roland Backhouse

3rd December, 2002

Fusion

Many problems are expressed in the form

$$\mathit{evaluate} \circ \mathit{generate}$$

where $\mathit{generate}$ generates a (possibly infinite) candidate set of solutions, and $\mathit{evaluate}$ selects a best solution.

Examples:

$$\mathit{shortest} \circ \mathit{path} \ ,$$

$$(x\in) \circ L \ .$$

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 $y \in A$,

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

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

$$-x \le y \;\equiv\; x \ge -y$$

$$x+y \le z \;\equiv\; y \le z-x$$

$$\lceil x \rceil \le n \equiv x \le n$$

$$x \uparrow y \le z \;\equiv\; x \le z \wedge y \le z$$

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

Examples — predicates

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

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

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

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

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

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

Examples — programming algebra

Languages ("factors")

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

$$L{\cdot}M \subseteq N \quad \equiv \quad M \subseteq L\backslash N$$

Relations ("residuals", "weakest pre and post specifications")

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

$$R{\circ}S \subseteq T \quad \equiv \quad S \subseteq R\backslash T$$

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

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

Strongest liberal postcondition

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

Hence

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

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

$$k \backslash m \wedge k \backslash n \;\equiv\; k \backslash \mathrm{gcd}(m, n) \quad ,$$

and least common multiple

$$m \backslash k \wedge n \backslash k \;\equiv\; \mathrm{lcm}(m, n) \backslash k \quad .$$

Definition of Infimum

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

$$\mathsf{x} :: \quad \langle \forall \mathsf{a} :: \mathsf{a} \sqsubseteq \mathsf{x} \equiv \langle \forall \mathsf{b} :: \mathsf{a} \sqsubseteq \mathsf{f.b} \rangle \rangle \quad . \tag{1}$$

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

$$\langle \forall \mathsf{a} \; :: \; \mathsf{a} \sqsubseteq \sqcap \mathsf{f} \equiv \langle \forall \mathsf{b} :: \mathsf{a} \sqsubseteq \mathsf{f.b} \rangle \rangle \quad .$$

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

Galois connection

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

$$
\begin{array}{ll}
 & \langle\forall b :: a \sqsubseteq f.b\rangle \\
\equiv & \{\quad \bullet \quad \text{define the function } \mathsf{K} \in (\mathcal{A}\leftarrow\mathcal{B})\leftarrow\mathcal{A} \text{ by } (\mathsf{K}.a).b = a \quad\} \\
 & \langle\forall b :: (\mathsf{K}.a).b \sqsubseteq f.b\rangle \\
\equiv & \{\quad \text{definition of } \dot{\sqsubseteq} \text{ (pointwise ordering on functions)} \quad\} \\
 & \mathsf{K}.a \mathrel{\dot{\sqsubseteq}} f\ .
\end{array}
$$

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

Definition of Supremum

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

$$x :: \quad \langle \forall a :: x \sqsubseteq a \equiv \langle \forall b :: f.b \sqsubseteq a \rangle \rangle \quad . \tag{2}$$

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,

$$\langle \forall a :: \sqcup f \sqsubseteq a \equiv \langle \forall b :: f.b \sqsubseteq a \rangle \rangle \quad . \tag{3}$$

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

$$\mathsf{f}.(\sqcap \mathsf{g}) = \sqcap(\mathsf{f} \bullet \mathsf{g}) \quad .$$

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

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

Examples

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

Hence,

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

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

Hence,

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

$$x \in S \Rightarrow b \quad \equiv \quad S \subseteq \textbf{if } b \textbf{ then } U \textbf{ else } U \backslash \{x\}$$

Hence,

$$x \in \cup \mathcal{S} \quad \equiv \quad \langle \exists P : P \in \mathcal{S} : x \in P \rangle$$

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

Hence,

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