Revision

Roland Backhouse

January 7, 2003

Outline

- Fixed Points
- Kleene Algebra
- Games
- Galois Connections
- Fixed Point Calculus
- Fusion

Fixed Points

$$\langle \text{Expression} \rangle \ ::= \ \langle \text{Expression} \rangle + \langle \text{Expression} \rangle \ \mid \ (\langle \text{Expression} \rangle) \ \mid \ \langle \text{Variable} \rangle$$

$$\begin{array}{lcl} fac.0 & = & 1 \\ fac.n & = & n * fac.(n-1), \text{ for } n > 0. \end{array}$$

$$\mathsf{List}\ a \ = \ \mathsf{Nil} \ \mid \ \mathsf{Cons}\ a\ (\mathsf{List}\ a)$$

$$\begin{array}{l} \mathsf{List}([\,])\ . \\ \mathsf{List}([X|Ys])\ :-\ \mathsf{List}(Ys)\ . \end{array}$$

Tarski's Theorem

A *fixed point* of an endofunction f is a value x such that

$$\mathsf{x} = \mathsf{f.x} \quad .$$

A *prefix point* of f is a value $\mathsf{x} \in \mathcal{A}$ such that

$$\mathsf{f.x} \leq \mathsf{x} \quad .$$

If f is a monotonic endofunction on the partially ordered set $(\mathcal{A}\,,\,\leq)$, the least fixed point of f equals the least prefix point of f.

The least prefix point of f is denoted by $\mu\mathsf{f}$. It is characterized by the rules:

computation rule

$$\mu\mathsf{f} = \mathsf{f}.\mu\mathsf{f}$$

induction rule: for all $\mathsf{x} \in \mathcal{A}$,

$$\mu\mathsf{f} \leq \mathsf{x} \;\Leftarrow\; \mathsf{f.x} \leq \mathsf{x} \quad .$$

Kleene Algebra

Algebra of choice $(+)$, sequencing $(\cdot)$ and iteration $(^*)$.

	carrier	$+$	$\cdot$	0	1	$\leq$
Languages	sets of words	$\cup$	$\cdot$	ϕ	$\{\varepsilon\}$	$\subseteq$
Programming	binary relations	$\cup$	$\circ$	ϕ	id	$\subseteq$
Reachability	booleans	$\vee$	$\wedge$	false	true	$\Rightarrow$
Shortest paths	nonnegative reals	min	$+$	∞	0	$\geq$
Bottlenecks	nonnegative reals	max	min	0	∞	$\leq$

Iteration ("Kleene star")

$a^* \cdot b$ is a fixed point of the function mapping x to $b + a{\cdot}x$:

$$b + a{\cdot}(a^*{\cdot}b) = a^*{\cdot}b \quad ,$$

and is the least among all prefix points of the function:

$$a^*{\cdot}b \leq x \quad \Leftarrow \quad b + a{\cdot}x \leq x \quad .$$

$b \cdot a^*$ is a fixed point of the function mapping x to $b + x{\cdot}a$:

$$b + (b{\cdot}a^*){\cdot}a = b{\cdot}a^* \quad ,$$

and is the least among all prefix points of the function:

$$b{\cdot}a^* \leq x \quad \Leftarrow \quad b + x{\cdot}a \leq x \quad .$$

Graph Problems

Suppose $\mathbf{A}$ is a square matrix representing the edges in a labelled graph. Suppose the edge labels are elements of a Kleene algebra.

$\mathbf{A}^*$ represents paths through the graph $\mathbf{A}$ of arbitrary (finite) edge length.

The (i,j)th element of $\mathbf{A}^*$ is the Kleene sum over all finite-length paths p from node i to node j of the weight of path p (the Kleene product of the path's edge labels).

Applications: reachability, shortest paths, bottleneck problems.

Kleene algebra is used in derivation of path-finding algorithms (eg the Warshall-Roy-Floyd algorithm).

Games

Used to illustrate least and greatest fixed points.

A two-person, impartial game is given by a set of *positions* and a *move* relation on the positions.

Let $W.\mathsf{G}$ mean that G is a position from which a perfect player is guaranteed to win.

Let $\mathsf{L}.\mathsf{G}$ mean that G is a position from which losing is inevitable (against a perfect player).

The predicates W and L satisfy the fixed point equations:

$$W \;=\; \langle \mathsf{G} \;::\; \langle \exists \mathsf{H} : \mathsf{G} \mapsto \mathsf{H} : \mathsf{L}.\mathsf{H} \rangle \rangle$$

$$\mathsf{L} \;=\; \langle \mathsf{G} \;::\; \langle \forall \mathsf{H} : \mathsf{G} \mapsto \mathsf{H} : W.\mathsf{H} \rangle \rangle$$

Winning, Losing and Stalemate

Consider the predicate transformers

$$f \;=\; \langle X :: \langle G :: \langle \exists H : G \mapsto H : X.H \rangle\rangle\rangle$$

and

$$g \;=\; \langle X :: \langle G :: \langle \forall H : G \mapsto H : X.H \rangle\rangle\rangle$$

defined by an impartial game.

f and g are *conjugates*. That is, for all predicates X,

$$\neg(f.X) \;=\; g.(\neg X) \quad \wedge \quad \neg(g.X) \;=\; f.(\neg X)$$

The predicates $\mu(f\bullet g)$, $\mu(g\bullet f)$ and $\nu(f\bullet g) \wedge \nu(g\bullet f)$ are mutually distinct and together cover all positions.

$\mu(f\bullet g)$ characterises the positions from which a win is guaranteed.

$\mu(g\bullet f)$ characterises the positions from which losing is inevitable.

$\nu(f\bullet g) \wedge \nu(g\bullet f)$ characterises stalemate positions.

(All these assume perfect players.)

Galois Connections

Many problems are expressed in the form

$$evaluate \circ generate$$

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

Function $evaluate$ is often a Galois connection, and $generate$ is often a fixed point.

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 $y \in A$,

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

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 $y \in A$, $x \preceq G.y \Rightarrow F.x \sqsubseteq y$.

Example. Read

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

as "the ceiling of x is the least (integer) n such that x is at most n".

Fixed Point Calculus

(Need a calculus because specifications are not implementations.)

computation rule

$$\mu f = f.\mu f$$

induction rule: for all $x \in \mathcal{A}$,

$$\mu f \le x \;\Leftarrow\; f.x \le x \quad .$$

closure rules

$$a^* \;=\; \langle \mu x :: 1 + x \cdot a \rangle \;=\; \langle \mu x :: 1 + a \cdot x \rangle \;=\; \langle \mu x :: 1 + a + x \cdot x \rangle$$

$$a^+ \;=\; \langle \mu x :: a + x \cdot a \rangle \;=\; \langle \mu x :: a + a \cdot x \rangle \;=\; \langle \mu x :: a + x \cdot x \rangle$$

rolling rule:

$$\mu(f \circ g) = f.\mu(g \circ f) \quad .$$

square rule:

$$\mu f = \mu(f^2) \quad .$$

diagonal rule:

$$\langle \mu x :: x \oplus x \rangle \;=\; \langle \mu x :: \langle \mu y :: x \oplus y \rangle \rangle \quad .$$

Fusion

$$F.(\mu_{\preceq} g) \;=\; \mu_{\sqsubseteq} h$$

provided that

- F is a lower adjoint in a Galois connection of $\sqsubseteq$ and $\preceq$ (see brief summary of definition below)
- $F \circ g \;=\; h \circ F$.

Example

For arbitrary language L,

$$\#\mathsf{L} \;=\; \langle \Downarrow w : w \in \mathsf{L} : \mathsf{length}.w \rangle$$

Because $\#$ is the infimum of the length function it is the lower adjoint in a Galois connection. Indeed,

$$\#\mathsf{L} \geq \mathsf{k} \;\equiv\; \mathsf{L} \subseteq \Sigma^{\geq \mathsf{k}}$$

where $\Sigma^{\geq \mathsf{k}}$ is the set of all words (in the alphabet Σ) whose length is at least k.

$$\# \langle \mu \mathsf{X} :: \{\mathsf{a}\} \cdot \mathsf{X} \cup \mathsf{X} \cdot \mathsf{X} \cup \{\varepsilon\} \rangle \;=\; \langle \mu \mathsf{k} :: (1+\mathsf{k}) \downarrow (\mathsf{k}+\mathsf{k}) \downarrow 0 \rangle \quad .$$

(Crucial step: $\#(\mathsf{Y} \cdot \mathsf{Z}) = \#\mathsf{Y} + \#\mathsf{Z}$.)

Problem Generalisation

Problem: For given grammar G, determine whether all words in $\mathsf{L(G)}$ have even length. I.e. implement

$$\mathsf{alleven} \circ \mathsf{L} \ .$$

The function $\mathsf{alleven}$ is a lower adjoint in a Galois connection. Specifically, for all languages S and T,

$$\mathsf{alleven(S)} \Leftarrow \mathsf{b} \quad \equiv \quad \mathsf{S} \subseteq \mathsf{if}\ \neg \mathsf{b} \rightarrow \Sigma^* \ \square\ \mathsf{b} \rightarrow (\Sigma \cdot \Sigma)^* \ \mathsf{fi}$$

Nevertheless, fusion *doesn't* work (directly) because

- there is no $\otimes$ such that, for all languages S and T,

$$\mathsf{alleven(S \cdot T)} \quad \equiv \quad \mathsf{alleven(S)} \otimes \mathsf{alleven(T)} \quad .$$

Solution: Generalise by tupling: compute simultaneously $\mathsf{alleven}$ and allodd.

Summary

- Algebraic properties key to efficient algorithms
- Calculation key to correct-by-construction
- Creativity still necessary.