Introduction to Kleene Algebras

Riccardo Pucella

Basic Notions Seminar

December 1, 2005

Idempotent Semirings

An *idempotent semiring* is a structure $\mathcal{S} = (S, +, \cdot, 1, 0)$ satisfying:

$$a + (b + c) = (a + b) + c$$

$$a + b = b + a$$

$$a + a = a$$

$$a + 0 = 0 + a = a$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

$$a \cdot 1 = 1 \cdot a = a$$

$$0 \cdot a = a \cdot 0 = 0$$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

They Are Not Rings!

The theory distinct from that of rings

- if R is an idempotent semiring such that every element has an additive inverse, then $a = 0$ for all a
- $a = a + 0 = a + a + a^{-1} = a + a^{-1} = 0$

Some Properties

Conventions

- ab for $a \cdot b$
- $a^n = a \cdot \cdots \cdot a$ (n times)

Well-defined partial order $\leq$ induced by $+$

- $x \leq y$ iff $x + y = y$
- $+$ and $\cdot$ monotone with respect to $\leq$

Relational Semirings

Let X be a set

The set of all binary relations on X forms an idempotent semiring under:

$$R + S \triangleq R \cup S$$

$$R \cdot S \triangleq S \circ R = \{(x, z) \mid \exists y \in X.(x, y) \in R, (y, z) \in S\}$$

$$0 \triangleq \varnothing$$

$$1 \triangleq id_X$$

The induced ordering is just subset inclusion

Kleene Algebras

A *Kleene algebra* is a structure $\mathcal{K} = (K, +, \cdot, ^*, 0, 1)$ where

- $(K, +, \cdot, 0, 1)$ is an idempotent semiring
- The * operation satisfies

$$1 + xx^* \leq x^*$$

$$1 + x^*x \leq x^*$$

$$b + ax \leq x \longrightarrow a^*b \leq x$$

$$b + xa \leq x \longrightarrow ba^* \leq x$$

The axioms say that a^*b is the unique least solution to $b + ax \leq x$

- Captures the notion of *iteration*

Relational Kleene Algebras

Relational semiring are Kleene algebras under:

$$R^* \triangleq \cup_{n \geq 0} R^n$$

In other words, R^* is the reflexive transitive closure of R

Boolean Algebras

Every Boolean algebra $\mathcal{B} = (B, \wedge, \vee, \bar{\ }, 0, 1)$ is a Kleene algebra under

$$a + b \triangleq a \vee b$$

$$a \cdot b \triangleq a \wedge b$$

$$a^* \triangleq 1$$

$$0 \triangleq 0$$

$$1 \triangleq 1$$

Formal Languages

Fix a set Σ of symbols
A *string* is a finite sequence of symbols from Σ
A *language* is a set of strings
The set of languages forms a Kleene algebra under

$$A + B \triangleq A \cup B$$

$$A \cdot B \triangleq \{xy \mid x \in A, y \in B\}$$

$$A^* \triangleq \cup_{n \geq 0} A^n = \{x_1 \ldots x_n \mid n \geq 0, x_i \in A\}$$

$$0 \triangleq \varnothing$$

$$1 \triangleq \{\epsilon\}$$

(where ϵ is the empty string)

Formal Languages, II

Take the smallest set of languages that:

- contains all singletons $\{x\}$ for $x \in \Sigma$
- contains $\varnothing$ and $\{\epsilon\}$
- is closed under $+, \cdot, ^*$

This is the *free Kleene algebra* generated by Σ

These are exactly the regular sets over Σ

- Sets of strings recognizable by finite state machines

The Tropical Algebra

Not all Kleene algebras are isomorphic to relational Kleene algebras.

Take $\mathbb{R}_+$, the nonnegative reals, extended with ∞ in the usual way. This forms a Kleene algebra under

$$
\begin{aligned}
a + b &= \min\{a, b\} \\
a \cdot b &= a +_{\mathbb{R}} b \\
a^* &= 0_{\mathbb{R}} \\
0 &= \infty \\
1 &= 0_{\mathbb{R}}
\end{aligned}
$$

Does not satisfy $a \leq 1 \longrightarrow a^2 = a$

Matrix Kleene Algebras

Given a Kleene algebra $\mathcal{K}$, the set of all $n \times n$ matrices over $\mathcal{K}$ forms a Kleene algebra $Mat_n(\mathcal{K})$ under the usual matrix operations, with * given inductively as follows:

$$\begin{bmatrix} a \end{bmatrix}^* \triangleq \begin{bmatrix} a^* \end{bmatrix}$$

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}^* \triangleq \begin{bmatrix} F^* & F^*BD^* \\ D^*CF^* & D^* + D^*CF^*BD^* \end{bmatrix}$$

where $F = A + BD^*C$

Application 1

All-pairs shortest path problem

Given a directed graph G with edge weights (say, representing distances between nodes)

Want to compute the length of the shortest path between all pairs of nodes efficiently

Step 1

Construct the adjacency matrix E, where E_{ij} is the edge distance between node i and node j, or ∞ if there is no edge from i to j

Application 1

All-pairs shortest path problem

Given a directed graph G with edge weights (say, representing distances between nodes)

Want to compute the length of the shortest path between all pairs of nodes efficiently

Step 2

Consider E as an element of $Mat_n(\mathbb{R}_+)$ and compute E^*

Application 1

All-pairs shortest path problem

Given a directed graph G with edge weights (say, representing distances between nodes)

Want to compute the length of the shortest path between all pairs of nodes efficiently

Step 3

Read off result: $(E^*)_{ij}$ is the length of the shortest path from node i to node j (∞ is no path exists)

Application 2

Equational reasoning about programs

Can think of a *program* as a way to describe actions to perform

Two programs are *equivalent* if they can perform the same sequences of actions

Equivalence is useful to establish correctness of program transformations

A Simple Programming Language

Let A be a set of primitive actions

Grammar of a simple nondeterministic programming language:

$$\begin{array}{rcl} S & ::= & a \in A \\ & & S_1; S_2 \\ & & S_1 \textbf{ or } S_2 \\ & & S^* \end{array}$$

E.g., $(a; b)^*; a$

Semantics

We associate to every program the *set of execution traces* that corresponds to executing the program

We use the fact that sets of strings form a Kleene algebra

$$[\![a]\!] \triangleq \{a\}$$

$$[\![S_1; S_2]\!] \triangleq [\![S_1]\!] \cdot [\![S_2]\!]$$

$$[\![S_1 \textbf{ or } S_2]\!] \triangleq [\![S_1]\!] + [\![S_2]\!]$$

$$[\![S^*]\!] \triangleq [\![S]\!]^*$$

Can equationally establish that $(a; b)^*; a$ and $a; (b; a)^*$ are equivalent programs

Kleene Algebras with Tests

As a programming language, the previous language is limited — there are no conditionals

Consider a special class of Kleene algebras

A *Kleene algebra with tests* is a Kleene algebra such that

- there exists $B \subseteq \{x \mid x \leq 1\}$
- B forms a Boolean algebra with $+, \cdot, 1, 0$ as $\vee, \wedge, 1, 0$

Formal Languages, III

Let Σ be a set of symbols

Let P be a set of primitive tests

let $\mathcal{B}_P$ be the free Boolean algebra generated by P

The set of languages over Σ and $\mathcal{B}_P$ forms a Kleene algebra with tests

- The embedded Boolean algebra consists of $\{b\}$ for $b \in \mathcal{B}_P$
- We identify $\wedge, \vee, 1, 0$ and $\cdot, +, 1, 0$

Another Programming Language

Let A be a set of primitive actions
Let P be a set of primitive tests

Grammar of a nondeterministic programming language:

$$
\begin{array}{rcl@{\qquad\qquad}rcl}
T & ::= & p & S & ::= & a \\
& & \neg T & & & S_1 ; S_2 \\
& & T_1 \wedge T_2 & & & \textbf{if } T \textbf{ then } S_1 \textbf{ else } S_2 \\
& & T_1 \vee T_2 & & & \textbf{while } T \textbf{ do } S
\end{array}
$$

Semantics

We give a semantics using sets of strings, this time relying on the fact that we have a Kleene algebra with tests

Tests T get mapped to elements of the embedded Boolean algebra

$$\begin{aligned} [\![p]\!] &\triangleq \{p\} \\ [\![\neg T]\!] &\triangleq \overline{[\![T]\!]} \\ [\![T_1 \wedge T_2]\!] &\triangleq [\![T_1]\!] \cdot [\![T_2]\!] \\ [\![T_1 \vee T_2]\!] &\triangleq [\![T_1]\!] + [\![T_2]\!] \end{aligned}$$

Semantics

We give a semantics using sets of strings, this time relying on the fact that we have a Kleene algebra with tests

Statements get mapped to sets of strings

$$\llbracket a \rrbracket \triangleq \{a\}$$

$$\llbracket S_1; S_2 \rrbracket \triangleq \llbracket S_1 \rrbracket \cdot \llbracket S_2 \rrbracket$$

$$\llbracket \textbf{if } T \textbf{ then } S_1 \textbf{ else } S_2 \rrbracket \triangleq (\llbracket T \rrbracket \cdot \llbracket S_1 \rrbracket) + (\overline{\llbracket T \rrbracket} \cdot \llbracket S_2 \rrbracket)$$

$$\llbracket \textbf{while } T \textbf{ do } S \rrbracket \triangleq (\llbracket T \rrbracket \cdot \llbracket S \rrbracket)^* \cdot \overline{\llbracket T \rrbracket}$$

Closing Remarks

Classification results?

- Standard decomposability questions
- In how many ways can you derive a Kleene algebra from an idempotent semiring?

Representation theorems?

- Under what conditions is a Kleene algebra isomorphic to a relational Kleene algebra?
- Is there a natural representation for all Kleene algebras?