Kleene Algebra and Arden's Theorem

Anshul Kumar
Inzemamul Haque

Motivation

- Regular Expression is a Kleene Algebra.
- We can use the properties and theorems of Kleene Algebra to simplify regular expressions
- We can use Kleene Algebra to find an equivalent regular expression for a DFA

Semi-group and Monoid

A semi-group is an algebraic structure (S, *), where S is a set and * is an associative binary operation on S.

A monoid is an algebraic structure (M, ., 1), where M is a set, . is an associative binary operation on M and 1 is the identity for . (i.e. $1.x=x.1=x$ for all $x \in M$).

A commutative monoid is a monoid in which

$$x \,.\, y = y \,.\, X$$

Note : Here 1 is just a symbol to represent identity element.

Examples

Set of natural numbers $\mathbb{N}$ with operation multiplication is a semi-group because multiplication of natural numbers is associative

Set of natural numbers $\mathbb{N}$ with operation addition is a monoid because addition of natural numbers is associative and there exists an identity element 0 (i.e. $x + 0 = 0 + x = x$ for every $x \in \mathbb{N}$).

Semi-ring

A semi-ring is an algebraic structure (S, +, ., 0, 1) such that

- (S, +, 0) is a commutative monoid
- (S, ., 1) is a monoid
- . distributes over + on both left and right

  i.e.

  $x \cdot (y + z) = x \cdot y + x \cdot z$ and

  $(x + y) \cdot z = x \cdot z + y \cdot z$
- 0 is an annihilator for .

  i.e. $x \cdot 0 = 0 \cdot x = 0$ for all x

A semi-ring is idempotent if $x + x = x$ for all x.

What is Kleene Algebra?

An algebraic structure (K, +, ., *, 0, 1) such that

- (K, +, ., 0, 1) is an idempotent semi-ring
- $1 + xx^* \leq x^*$
- $1 + x^*x \leq x^*$
- $b + ax \leq x \rightarrow a^*b \leq x$
- $b + xa \leq x \rightarrow ba^* \leq x$

where

$$a \leq b \leftrightarrow a + b = b$$

It can be shown that ≤ is partial order.

$\leq$ is a partial order (1)

Reflexive –

Since K is an idempotent semiring, hence

$a + a = a$

$\Rightarrow$ $a \leq a$

$\Rightarrow$ Hence $\leq$ is reflexive

Anti-Symmetric –

$a \leq b$ and $b \leq a$

$\Rightarrow$ $a + b = b$ and $b + a = a$

$\Rightarrow$ $a + b = b$ and $a + b = a$ [Since K is a semi-ring hence + is commutative]

$\Rightarrow$ $a = b$

Hence $\leq$ is anti-symmetric

$\leq$ is a partial order (2)

Transitive –

$a \leq b$ and $b \leq c$

$\Rightarrow$ $a + b = b$ and $b + c = c$

$\Rightarrow$ $(a + b) + c = c$ [Since $a + b = b$]

$\Rightarrow$ $a + (b + c) = c$ [+ is associative]

$\Rightarrow$ $a + c = c$ [Since $b + c = c$]

$\Rightarrow$ $a \leq c$

Hence $\leq$ is transitive

Hence $\leq$ is a partial order.

Examples of Kleene-Algebra (1)

Boolean Algebra (B, ^, ˅, , 0, 1) is a Kleene Algebra under

$$a + b \equiv a \lor b$$

$$a \,.\, b \equiv a \land b$$

$$a^* \equiv 1$$

$$0 \equiv 0$$

$$1 \equiv 1$$

Examples of Kleene-Algebra (2)

The set of languages forms a Kleene Algebra under

$$A + B \equiv A \cup B$$

$$A \,.\, B \equiv \{ xy \mid x \in A, y \in B \}$$

$$A^* \equiv \bigcup_{n \geq 0} A^n$$

$$0 \equiv \phi$$

$$1 \equiv \{\epsilon\}$$

Some typical Theorems of Kleene-Algebra

$$a^*a^* = a^*$$

$$a^{**} = a^*$$

$$(a^*b)^*a^* = (a+b)^*$$ denesting rule

$$a(ba)^* = (ab)^*a$$ shifting rule

$$a^* = (aa)^* + a(aa)^*$$

Matrices over Kleene-Algebra (1)

Given an arbitrary Kleene Algebra K, the set of n x n matrices over K denoted by M(n,K) also form Kleene Algebra.

In general, + and . are ordinary matrix addition and multiplication respectively.

Identity for + is zero matrix

Identity for . is identity matrix

E* is defined by induction on n for an n x n matrix over K.

Matrices over Kleene-Algebra (2)

Definition of E*

If n=1, M(n,K) = K, we already know * for K

For n>1, break E up into four submatrices

$$E = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

E* is defined as

$$E^* = \begin{bmatrix} (A + BD^*C)^* & (A + BD^*C)^*BD^* \\ (D + CA^*B)^*CA^* & (D + CA^*B)^* \end{bmatrix}$$

Arden's Theorem (1)

Statement:

In any Kleene Algebra, a^*b is the ≤-least solution of the equation $x = ax + b$.

As we know that set of languages under the operation union and concatenation is also a Kleene Algebra.

Hence Arden's theorem can also be stated in terms of languages as:

$A^*\cdot B$ is the smallest language that is a solution for X in the linear equation $X = A\cdot X \cup B$ where X, A, B are sets of strings. Moreover, if the set A does not contain the empty word, then this solution is unique.

Arden's Theorem (2)

Note: This proof is not correct. But you can get some idea from this

Proof:

It can be easily shown that a^*b is the solution of the equation $x = ax + b$ because it satisfies the given equation.

Let c be any solution to $x = ax + b$

Thus we have to show that $a^*b \leq c$ for every solution c

Arden's Theorem (3)

Since c is the solution to x = ax + b, c satisfies the given equation

i.e. $c = ac + b$

Hence $c \leq ac + b$ (1)

and $ac + b \leq c$ (2)

Hence from (2),

$ac \leq c$ and $b \leq c$

$b \leq c \Rightarrow ab \leq ac$ but $ac \leq c$

$\Rightarrow ab \leq c$

Similarly we can show $aab \leq c$, $aaab \leq c$,… and so on

Hence it can be shown that $a^*b \leq c$

References

- Dexter Kozen, Automata and Computability, Springer
- Dexter Kozen, Lecture-2, Introduction to Kleene Algebra, http://www.cs.cornell.edu/Courses/cs786/2004sp/Lectures/l02-axioms.pdf
- Dexter Kozen, Lecture-7, Introduction to Kleene Algebra, http://www.cs.cornell.edu/Courses/cs786/2004sp/Lectures/l07-complete.pdf
- Riccardo Pucella, Introduction to Kleene Algebra, www.ccs.neu.edu/home/**riccardo**
- Dan Dougherty, CS-503 Lecture Notes, http://web.cs.wpi.edu/~dd/courses/503/

Queries