Introduction to Kleene Algebra **Lecture 2**
CS786 Spring 2004 **January 28, 2004**

Axioms of Kleene Algebra

In this lecture we give the formal definition of a Kleene algebra and derive some basic consequences.

Semigroups and Monoids

A *semigroup* is an algebraic structure $(S,\ \cdot)$, where S is a set and $\cdot$ is an associative binary operation on S, which means that $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in S$. This allows us to write $x \cdot y \cdot z$ without ambiguity. A *monoid* is an algebraic structure $(M,\ \cdot,\ 1)$ where $(M,\ \cdot)$ is a semigroup and 1 is a distinguished element of M that is both a left and right identity for $\cdot$ in the sense that $1 \cdot x = x \cdot 1 = x$ for all $x \in M$.

For semigroups and monoids written multiplicatively, we often omit the operator $\cdot$ in expressions, writing xy for $x \cdot y$.

Example 2.1 The following are common examples of monoids:

1. $(\Sigma^*,\ \cdot,\ \varepsilon)$, where Σ^* is the set of finite-length strings over an alphabet Σ, $\cdot$ is concatenation of strings, and ε is the null string;

2. $(2^{\Sigma^*},\ \cdot,\ \{\varepsilon\})$, where $\cdot$ is set concatenation as described in the last lecture;

3. $(2^{\Sigma^*},\ \cup,\ \varnothing)$, where 2^{Σ^*} is the powerset or set of all subsets of Σ^*, $\cup$ is set union, and $\varnothing$ is the empty set;

4. $(\mathbb{N},\ +,\ 0)$, where $\mathbb{N}$ is the set of natural numbers $\{0, 1, 2, \ldots\}$;

5. $(\mathbb{N},\ \cdot,\ 1)$;

6. $(\mathbb{N}^n,\ +,\ \overline{0})$, where $\mathbb{N}^n$ is the Cartesian product of n copies of $\mathbb{N}$, $+$ is vector addition, and $\overline{0}$ is the zero vector;

7. $(\mathbb{R}_+ \cup \{\infty\},\ \min,\ \infty)$, where $\mathbb{R}_+$ denotes the set of nonnegative real numbers, ∞ is a special infinite element greater than all real numbers, and min gives the minimum of two elements;

8. $(R^{n\times n},\ \cdot,\ I)$, where $R^{n\times n}$ denotes the set of $n \times n$ matrices over a ring R, $\cdot$ is ordinary matrix multiplication, and I is the identity matrix;

9. $(X \to X,\ \circ,\ \iota)$, where $X \to X$ denotes the set of all functions from a set X to itself, $\circ$ is function composition, and ι is the identity function.

□

Examples 3–7 are *commutative* monoids, which means that $xy = yx$ for all x, y. Example 8 is never commutative for any nontrivial ring R and $n \geq 2$. Example 9 is never commutative for any X with at least 2 elements.

Idempotent Semirings

A *semiring* is an algebraic structure $(S,\ +,\ \cdot,\ 0,\ 1)$ such that

- $(S,\ +,\ 0)$ is a commutative monoid,
- $(S,\ \cdot,\ 1)$ is a monoid,
- $\cdot$ distributes over $+$ on both the left and right in the sense that $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$,
- 0 is an *annihilator* for $\cdot$ in the sense that $0 \cdot x = x \cdot 0 = 0$ for all x.

A semiring is *idempotent* if $x + x = x$ for all x. We often abbreviate $x \cdot y$ to xy, and avoid parentheses by taking $\cdot$ to be higher precedence than $+$.

Collecting these axioms, we define an *idempotent semiring* to be any structure $(S, +, \cdot, 0, 1)$ satisfying the following identities for all $x, y, z \in S$:

$$\begin{array}{ll}
x + (y + z) = (x + y) + z & x + y = y + x \\
x + 0 = x & x + x = x \\
x(yz) = (xy)z & 1x = x1 = x \\
x(y + z) = xy + xz & (x + y)z = xz + yz \\
0x = x0 = 0. &
\end{array}$$

A *ring* is a semiring in which the additive monoid forms a group; that is, in which additive inverses exist. We cannot have additive inverses in an idempotent semiring unless the semiring is trivial, since $0 = -x + x = -x + x + x = 0 + x = x$.

Order

Recall that a *partial order* is a binary relation on a set that is

- reflexive: for all x, $x \leq x$,
- antisymmetric: for all x, y, if $x \leq y$ and $y \leq x$, then $x = y$, and
- transitive: for all x, y, z, if $x \leq y$ and $y \leq z$, then $x \leq z$.

Any idempotent semiring has a naturally-defined partial order $\leq$ associated with it:

$$x \leq y \quad \overset{\text{def}}{\iff} \quad x + y = y. \tag{1}$$

The order relation $\leq$ is so central to the theory that one might take it as primitive, but we will consider it an abbreviation for the equation on the right-hand side of (1).

In the language-theoretic and relational models of the last lecture, $\leq$ is set inclusion $\subseteq$. But beware: in the min, + algebra, $\leq$ is the *reverse* of the natural order on $\mathbb{R}$ extended to $\mathbb{R}_+ \cup \{\infty\}$. By (1), $x \leq y$ iff $\min x, y = y$, but this occurs iff x is greater than or equal to y in the natural order on $\mathbb{R}$. (Note that we are carefully avoiding the use of the notation $\leq$ for the natural order on $\mathbb{R}$!)

That $\leq$ is a partial order follow easily from the definition (1) and the axioms of idempotent semirings. Reflexivity is just the idempotence axiom $x + x = x$. Antisymmetry follows from commutativity of +: if $x \leq y$ and $y \leq x$, then $y = x + y = y + x = x$. Finally, for transitivity, if $x \leq y$ and $y \leq z$, then

$$\begin{aligned}
x + z &= x + (y + z) && \text{since } y + z = z \\
&= (x + y) + z && \text{associativity of } + \\
&= y + z && \text{since } x + y = y \\
&= z && \text{again since } y + z = z,
\end{aligned}$$

therefore $x \leq z$.

In any idempotent semiring, the operators + and $\cdot$ are *monotone* with respect to $\leq$ in the sense that for all $x, y, z \in S$,

$$\begin{aligned}
x \leq y &\rightarrow x + z \leq y + z \\
x \leq y &\rightarrow z + x \leq z + y \\
x \leq y &\rightarrow xz \leq yz \\
x \leq y &\rightarrow zx \leq zy.
\end{aligned}$$

(Monotonicity will also hold for the * operator of Kleene algebra, that is, $x \leq y \rightarrow x^* \leq y^*$, when we get around to discussing it.) These properties follow easily from the axioms.

In any idempotent semiring, the operator $+$ gives the *least upper bound* or *supremum* of any pair of elements with respect to the natural order $\leq$, and 0 is the least element of the semiring with respect to $\leq$. To say that $x + y$ is the *least upper bound* of x and y says that

- $x \leq x + y$ and $y \leq x + y$ ($x + y$ is an upper bound for x and y);
- if z is any other upper bound, that is, if $x \leq z$ and $y \leq z$, then $x + y \leq z$ ($x + y$ is the *least* upper bound).

The proof that $x + y$ is an upper bound uses associativity and idempotence: $x + (x + y) = (x + x) + y = x + y$, and similarly for $y \leq x + y$. The proof that it is the least upper bound uses only associativity: if $x \leq z$ and $y \leq z$, then $(x + y) + z = x + (y + z) = x + z = z$.

One observation that is not difficult to check is that the $n \times n$ matrices over a semiring again form a semiring under the natural definitions of the matrix operations. Moreover, if the underlying semiring is idempotent, then so is the matrix semiring (Exercise **??**).

The * Operator

Now we turn to the * operator. This is the most interesting part of Kleene algebra, because it captures the notion of *iteration.* Because of this, it may seem that * is inherently infinitary. Indeed, there are several infinitary axiomatizations that we will consider. However, it is possible to derive most of the interesting parts of the theory in a purely finitary way.

The * operator is a unary operator written in postfix. Intuitively, x^* represents zero or more iterations of x. In relational models, this is reflexive transitive closure; in language models, the Kleene asterate.

There are several different competing axiomatizations of *, and in part our study will be to understand the relationships among them. For now, we shall pick a particular one as our official definition for the purposes of this course. Thus we define a *Kleene algebra* to be a structure $(K, +, \cdot, ^*, 0, 1)$ that is an idempotent semiring under $+, \cdot, 0, 1$ satisfying the properties (2)–(5) below. We assign precedence $^* > \cdot > +$ to the operators to avoid unnecessary parentheses.

The axioms for * consist of two equations and two equational implications or *Horn formulas.* (Note that up to now, the axioms have been purely equational.) The two equational axioms for * are

$$\begin{aligned} 1 + xx^* &\leq x^* & (2)\\ 1 + x^*x &\leq x^* & (3)\end{aligned}$$

and the two equational implications are

$$\begin{aligned} b + ax \leq x &\rightarrow a^*b \leq x & (4)\\ b + xa \leq x &\rightarrow ba^* \leq x. & (5)\end{aligned}$$

Of course, these are all considered to be implicitly universally quantified, so that (4) and (5) are assumed to hold for all a, b, and x in any Kleene algebra.

The significance of (2)–(5) concerns the solution of linear inequalities. As we shall see, much of the theory of Kleene algebra is concerned with the solution of finite systems of linear inequalities. For example, a finite automaton is essentially such a system. Axioms (2) and (4) provide for the existence of a unique least solution to a certain single linear inequality in a single variable, namely

$$b + aX \quad \leq \quad X, \tag{6}$$

where X is a variable ranging over elements of the Kleene algebra. Axioms (2) and (4) together essentially say that a^*b is a solution to (6), and moreover, it is the unique least solution among all solutions in the Kleene algebra. First, (2) says that a^*b is a solution, since by monotonicity of multiplication and distributivity,

$$\begin{aligned} 1 + aa^* \leq a^* \quad &\rightarrow \quad (1 + aa^*)b \leq a^*b \\ &\rightarrow \quad b + a(a^*b) \leq a^*b \ ; \end{aligned}$$

and (4) says exactly that a^*b is less than or equal to any other solution, therefore it is the unique least solution. Dually, the axioms (3) and (5) say that ba^* is the unique least solution to $b + Xa \leq X$.

Let us illustrate the use of (4) and (5) to show that (2) and (3) can be strengthened to equalities. We show this for (2); the result for (3) is symmetric. We already have that $1 + xx^* \leq x^*$, so by antisymmetry, it suffices to show the reverse inequality; equivalently,

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

This is the right-hand side of (4) with 1 substituted for b, x substituted for a, and $1 + xx^*$ substituted for x, so it suffices to show that the left-hand side of (4) holds under the same substitution, or

$$1 + x(1 + xx^*) \quad \leq \quad 1 + xx^*.$$

But this is immediate from (2) and monotonicity.

Recall from the last lecture that in relational models, R^* was defined to be the reflexive transitive closure of the relation R. To be reflexive means that $\iota \subseteq R^*$, where ι is the identity relation; to be transitive means that $R^* \circ R^* \subseteq R^*$; and to contain R means that $R \subseteq R^*$. Abstractly, these properties are expressed by the inequalities

$$\begin{aligned} 1 &\leq x^* \qquad (7) \\ x^*x^* &\leq x^* \qquad (8) \\ x &\leq x^*, \qquad (9) \end{aligned}$$

respectively. Equivalently,

$$1 + x^*x^* + x \quad \leq \quad x^*. \tag{10}$$

We might interpret this inequality as saying that x^* is a reflexive and transitive element dominating x. It does not, however, say that it is the reflexive transitive closure of x; for that we need the equational implication

$$1 + yy + x \leq y \quad \rightarrow \quad x^* \leq y, \tag{11}$$

which says that x^* is the *least* reflexive and transitive element dominating x.

Now in the presence of the other axioms, (10) is equivalent to (2) (and, by symmetry, to (3) as well). To prove that (2) implies (10), it suffices to show that (2) implies (7)–(9). The inequality (7) is immediate from (2). Also, multiplying (7) on the left by x, by monotonicity we have $x \leq xx^*$; then (9) is immediate from this and (2). The last inequality (8) is left as an exercise (Homework 1, Exercise 1(a)). This argument requires either (4) or (5).

Conversely, to show that (10) implies (2), assume (10). Then $1 \leq x^*$ from (7). Also, by (8), (9), and monotonicity we have $xx^* \leq x^*x^* \leq x^*$. Since $1 + xx^*$ is the least upper bound of 1 and xx^*, we have (2).

Each of (4) and (5) alone implies (11). The converse does not hold: later, we will construct a "left-handed" Kleene algebra that is not "right-handed" (one satisfying (4) but not (5)). To show that (4) implies (11), suppose that (4) holds for all a, b, and x, and assume the left-hand side of (11). To show the right-hand side of (11) holds, by (4) it suffices to show that $1 + xy \leq y$. But this follows easily from the left-hand side of (11): we have $x \leq y$, and by monotonicity, $1 + xy \leq 1 + yy \leq y$.

In the presence of the other axioms, the implications (4) or (5) are equivalent to

$$ax \leq x \quad \rightarrow \quad a^*x \leq x \tag{12}$$

$$xa \leq x \quad \rightarrow \quad xa^* \leq x, \tag{13}$$

respectively. These alternative forms are quite useful in some contexts. The proofs of equivalence are left as an exercise (Exercise **??**).

Finally, as promised, we show that * is monotone. Suppose $x \leq y$. We wish to show that $x^* \leq y^*$. By (4), it suffices to show that $1 + xy^* \leq y^*$. But since $x \leq y$, by monotonicity and (2) we have $1 + xy^* \leq 1 + yy^* \leq y^*$.

Next time we will look at some alternative axiomatizations of *.