Kleene algebra (with tests)

Dynamic Logic – Lecture 2

Igor Sedlár

Institute of Computer Science of the Czech Academy of Sciences

Faculty of Arts, Charles University
Fall Semester 2023-24

Lecture overview

- Kleene algebra (KA) is a (quasi-equational) axiomatization of the algebra of regular languages
- Kleene algebra with tests (KAT) extends KA with a Boolean algebra of tests; typical models are relational and trace models (guarded languages)
- KAT allows to express all the expressions of the formal language of programs; KATs generalize the kinds of program models introduced in the previous lecture

Semirings – 1

Definition 1

A semiring is an algebra $\langle S, +, \cdot, 0, 1 \rangle$ *such that*

- $\langle S, +, 0 \rangle$ *is a commutative monoid*
- $\langle S, \cdot, 1 \rangle$ *is a monoid*
- $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ *and* $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
- $0 \cdot x = 0 = x \cdot 0$

A semiring is idempotent iff $x + x = x$, and complete if $\langle S, +, 0 \rangle$ is a complete monoid and

$$\sum_{i \in I} (x \cdot y_i) = x \cdot \left(\sum_{i \in I} y_i \right) \qquad \sum_{i \in I} (x_i \cdot y) = \left(\sum_{i \in I} x_i \right) \cdot y$$

In a complete idempotent semiring (unital quantale): $x^* := \sum_{n \geq 0} x^n$.

Semirings – 2

Examples

- Binary relations: $\langle 2^{X \times X}, \cup, \circ, \emptyset, 1_X \rangle$
- Formal languages: $\langle 2^{A^*}, \cup, \cdot, \emptyset, \{\epsilon\} \rangle$ where ϵ is the empty word and $K \cdot L = \{wu \mid w \in K \;\; \& \;\; u \in L\}$
- Sets of traces (over Σ and Π): $\langle 2^{Tr}, \cup, \diamond, \emptyset, \mathsf{States} \rangle$
- Tropical semiring: $\langle \mathbb{N} \cup \{\infty\}, \min, +, \infty, 0 \rangle$ where $\infty + n = \infty = n + \infty$ and $\min\{n, \infty\} = n$
- Boolean semiring: $\langle \{\mathsf{true}, \mathsf{false}\}, \vee, \wedge, \mathsf{false}, \mathsf{true} \rangle$

Exercise 1

Which examples above are idempotent? complete? What is * in the complete cases?

Kleene algebras – 1

Definition 2

A Kleene algebra is an algebra $\langle X, +, \cdot, {}^*, 0, 1\rangle$ expanding an idempotent semiring with a unary operation * satisfying:

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

$$y + zx \leq z \implies yx^* \leq z \qquad y + xz \leq z \implies x^*y \leq z$$

(where $x \leq y \iff x + y = y$ and xy is $x \cdot y$)

A Kleene algebra is *-continuous iff

$$xy^*z = \sum_{k \geq 0} xy^k z$$

for all x, y, z. (The sum is required to exist for all x, y, z by definition of KA*.)

Kleene algebras – 2

Proposition 1

*Every (unital) quantale is a *-continuous Kleene algebra.*

Proof (partial). We prove $1 + xx^* + x^* = x^*$:

$$x^0 + x \sum_{n \geq 0} x^n + \sum_{n \geq 0} x^n = x^0 + \sum_{n \geq 0} x^{n+1} + \sum_{n \geq 0} x^n$$

$$= \sum_{n \geq 0} x^n + \sum_{n \geq 0} x^n = \sum_{n \geq 0} x^n$$

□

Proposition 2

*Not every *-continuous KA is a unital quantale. Not every KA is *-continuous.*

Regular expressions – 1

Definition 3

Let Σ be an alphabet. The set $\mathbb{E}(\Sigma)$ of regular expressions over Σ is defined using the following grammar:

$$e, f := \mathsf{a} \in \Sigma \mid 0 \mid 1 \mid e + f \mid e \cdot f \mid e^*$$

Operator precedence: * over $\cdot$ over $+$. We'll sometimes write ef instead of $e \cdot f$. Hence, $ef^* + e$ is $(e \cdot (f^*)) + e$.

Definition 4

A Kleene algebra model is $\langle X, v \rangle$ where $X \in \mathsf{KA}$ and $v : \Sigma \to X$.

Every $\langle X, v \rangle$ extends to an interpretation $[\![-]\!]_v : \mathbb{E}(\Sigma) \to X$ (homomorphism).

An equation $e \approx f$ is valid in KA iff $[\![e]\!]_v = [\![f]\!]_v$ for all $\langle X, v \rangle$.

(Notation: $\mathsf{KA} \models e \approx f$, $e \overset{\mathsf{KA}}{\equiv} f$ or just $e \equiv f$).

Regular expressions – 2

Definition 5

The (canonical) language interpretation is $[\![-]\!] : \mathbb{E}(\Sigma) \to 2^{\Sigma^*}$ *such that*

$$[\![\mathtt{a}]\!] = \{\mathtt{a}\} \qquad [\![0]\!] = \emptyset \qquad [\![1]\!] = \{\epsilon\}$$

$$[\![e + f]\!] = [\![e]\!] \cup [\![f]\!] \quad [\![e \cdot f]\!] = [\![e]\!] \cdot [\![f]\!] \quad [\![e^*]\!] = \bigcup_{n \geq 0} [\![e]\!]^n = [\![e]\!]^*$$

A language $L \subseteq \Sigma^*$ *is regular iff there is* $e \in \mathbb{E}(\Sigma)$ *such that* $L = [\![e]\!]$*.*

Proof of Prop. 2, first part (hint). Show that the Kleene algebra of regular languages is *-continuous but not a (unital) quantale.

Proposition 3

A language $L \subseteq \Sigma^*$ *is regular iff it belongs to the closure of the set of finite subsets of* Σ^* *under the regular operations* $\cup, \cdot$ *and* **.*

Completeness

Theorem 1 (Kozen 1994)

KA $\models e \approx f$ *iff* $[\![e]\!] = [\![f]\!]$.

Proof (sketch). L⇒R: The algebra of regular languages is a Kleene algebra. R⇒L: Much more intricate and beyond our scope (see notes). □

Note: This is a completeness theorem for the algebra of regular languages since KA $\models e \approx f$ iff $e \approx f$ is derivable from the obvious quasi-equational axiomatization.

Kleene algebras with tests – 1

Definition 6

A <u>Kleene algebra with tests</u> is an algebra $\langle X, B, +, \cdot, {}^*, {}^-, 0, 1\rangle$ *where*

- $\langle X, +, \cdot, {}^*, 0, 1\rangle$ *is a Kleene algebra*
- $B \subseteq X$ *and* ${}^- : B \to B$ *(partial on* X*)*
- $\langle B, +, \cdot, {}^-, 0, 1\rangle$ *is a Boolean algebra.*

*A KAT is *-continuous iff its underlying KA is.*

Intuition: B is a collection of "tests", special actions among all the X. Tests pertain to Boolean statements, hence they form a Boolean algebra.

Kleene algebras with tests – 2

Examples

- Every KA ($B = \{0, 1\}$)
- Binary relations:
  $\langle 2^{X \times X}, 2^{1_X} \cup, \circ, {}^*, {}^-, \emptyset, 1_X \rangle$ where ${}^-$ is complement w.r.t. 1_X
- Formal languages: $\langle 2^{\Sigma^*}, \{\emptyset, \{\epsilon\}\}, \cup, \cdot, {}^*, {}^-, \emptyset, \{\epsilon\} \rangle$
- Sets of traces (over Σ and Π):
  $\langle 2^{Tr}, 2^{\mathsf{States}}, \cup, \diamond, {}^*, {}^-, \emptyset, \mathsf{States} \rangle$ where ${}^-$ is complement w.r.t. States.

Note: $Reg(\Sigma)$ forms a Boolean algebra, but $\wedge$ is $\cap$, not $\cdot$.

Regular expressions with tests – 1

Definition 7

Let Σ and Π be alphabets. The set $\mathbb{E}(\Sigma, \Pi)$ of regular expressions over Σ with tests over Π is defined using the following (two-sorted) grammar:

$$b, c := \mathtt{p} \in \Pi \mid b + c \mid b \cdot c \mid \overline{b} \mid 0 \mid 1$$

$$e, f := \mathtt{a} \in \Sigma \mid b \mid e + f \mid e \cdot f \mid e^*$$

We define:

$$\textbf{if } b \textbf{ then } e \textbf{ else } f := be + \overline{b}f \qquad \textbf{while } b \textbf{ do } e := (be)^*\overline{b}$$

Regular expressions with tests – 2

Definition 8

A <u>KAT model</u> is $\langle X, v\rangle$ *where* $X \in \mathsf{KAT}$ *and* $v : \Sigma \cup \Pi \to X$ *such that* $v(\mathrm{p}) \in B$ *for all* $\mathrm{p} \in \Pi$.

Every $\langle X, v\rangle$ *extends to an <u>interpretation</u>* $[\![-]\!]_v : \mathbb{E} \to X$ *(homomorphism).*

<u>Validity:</u> $\mathsf{KAT} \models e \approx f$ *iff* $[\![e]\!]_v = [\![f]\!]_v$ *for all* $\langle X, v\rangle$.

Exercise 2

Show that if X is a relational KAT or a KAT of traces, then the interpretation of $\mathbf{if}\ b\ \mathbf{then}\ e\ \mathbf{else}\ f$ and $\mathbf{while}\ b\ \mathbf{do}\ e$ induced by any $\langle X, v\rangle$ coincides with the relational and trace semantics of programs as defined in the previous lecture.

Regular expressions with tests – 3

We assume that Π is finite and comes with a fixed ordering: $\mathtt{p}_1, \ldots, \mathtt{p}_n$.

Definition 9

An atom over Π is a sequence $r_1 \ldots r_n$ where $r_i \in \{\mathtt{p}_i, \overline{\mathtt{p}}_i\}$. Let A be the set of all atoms over Π. A guarded string over Σ and Π is any word in $(A \cdot \Sigma)^* \cdot A$, that is, any sequence of the form

$$S_1 \mathtt{a}_1 S_2 \ldots \mathtt{a}_{n-1} S_n$$

where $S_i \in A$ over Π and $\mathtt{a}_j \in \Sigma$. Let GS be the set of all guarded strings (over Σ, Π).

We write $r_1 \ldots r_n \vDash \mathtt{p}_i$ iff $r_i = \mathtt{p}_i$.

Regular expressions with tests – 3

Fusion product $\diamond$ on guarded strings is defined in the expected way.

Definition 10

The (canonical) language interpretation is $[\![-]\!] : \mathbb{E} \to 2^{GS}$ *such that*

$$[\![\mathtt{p}]\!] = \{S \mid S \vDash \mathtt{p}\} \quad [\![0]\!] = \emptyset \qquad [\![1]\!] = A \quad [\![\bar{b}]\!] = A \setminus [\![b]\!]$$

$$[\![\mathtt{a}]\!] = \{S\mathtt{a}T \mid S, T \in A\}$$

$$[\![e + f]\!] = [\![e]\!] \cup [\![f]\!] \quad [\![e \cdot f]\!] = [\![e]\!] \diamond [\![f]\!] \quad [\![e^*]\!] = \bigcup_{n \geq 0} [\![e]\!]^n = [\![e]\!]^*$$

A guarded language $L \subseteq GS$ *is regular iff there is* $e \in \mathbb{E}$ *such that* $L = [\![e]\!]$.

Completeness

Theorem 2

The following are equivalent:

1. KAT $\models e \approx f$
2. KAT* $\models e \approx f$
3. rKAT $\models e \approx f$
4. $[\![e]\!] = [\![f]\!]$

Proof (sketch). 1⇒2⇒3 is trivial. 3⇒4 by a Caley construction: For $L \subseteq GS$, let

$$\mathsf{cay}(L) = \{\langle w, w \diamond u \rangle \mid w \in GS \;\; \& \;\; u \in L\}$$

The function cay is injective. We can prove by induction on e that $[\![e]\!]_{\langle X, v \rangle} = \mathsf{cay}\,([\![e]\!])$ for X the rKAT of binary relations on GS and $v(\mathtt{x}) = \mathsf{cay}\,([\![\mathtt{x}]\!])$ for $\mathtt{x} \in \Sigma \cup \Pi$.

4⇒1: It can be shown that for each e there is $\hat{e}$ such that (i) KAT $\models e \approx \hat{e}$ and $[\![e]\!] = [\![\hat{e}]\!]$ where $\hat{e}$ is seen as a regular expression over $\Sigma \cup \mathsf{Lit}(\Pi)$. $\mathsf{Lit}(\Pi)$ is the set of literals over Π. Then proceed using Theorem 1. □

Exercises

3. Finish the proof of Proposition 1.

4. Prove that x^* is the least prefixpoint of functions f, g such that $f(y) = 1 + xy$ and $g(y) = 1 + yx$.

5. Prove Proposition 3.

6. Show that KA $\models e \approx f$ iff KA* $\models e \approx f$ iff rKA $\models e \approx f$. (Where KA* is the class of *-continuous KA and rKA is the class of KA of binary relations.)

7. * Prove by induction of f that for all $e, g \in \mathbb{E}$ and all $\langle X, v \rangle$ where $X \in$ KAT*:

$$[\![efg]\!]_v = \sum_{w \in [\![f]\!]} [\![ewg]\!]_v$$

(note that each $w \in GS$ can be seen as an expression in $\mathbb{E}$). Infer from that that KAT $\models e \approx f$ iff KAT* $\models e \approx f$.

Notes

- The study of regular expressions and languages goes back to (Kleene, 1956)
- Kozen's completeness theorem is established in (Kozen, 1994). For an accessible overview, see Kappé's lecture notes (Kappé, 2023).
- Kozen (1990) gives an example of a Kleene algebra that is not *-continuous
- Kleene algebras with tests are introduced in (Kozen, 1997) where their utility in studying programs is discussed as well.
- Theorem 2 is established in (Kozen and Smith, 1997).

References

- Tobias Kappé. Elements of Kleene algebra. Course notes, ESSLLI 2023, 2023.
- Stephen C Kleene. Representation of events in nerve nets and finite automata. In C. E. Shannon and J. McCarthy, editors, *Automata Studies*, pages 3 – 41. Princeton University Press, 1956.
- Dexter Kozen. On Kleene algebras and closed semirings. In B. Rovan, editor, *International Symposium on Mathematical Foundations of Computer Science*, pages 26–47. Springer, 1990.
- Dexter Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366 – 390, 1994.
- Dexter Kozen. Kleene algebra with tests. *ACM Trans. Program. Lang. Syst.*, 19(3):427–443, May 1997.
- Dexter Kozen and Frederick Smith. Kleene algebra with tests: Completeness and decidability. In Dirk van Dalen and Marc Bezem, editors, *Computer Science Logic*, pages 244–259, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg.