

Dynamic Logic

Part 3: Kleene Algebra With Tests

Wolfgang Poiger and Igor Sedlár

Institute of Computer Science
Czech Academy of Sciences

Faculty of Arts, Charles University
Fall Semester 2025-26



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 first part of the course

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

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

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): $\langle 2^{Tr}, \cup, \diamond, \emptyset, \text{States} \rangle$
- Tropical semiring: $\langle \mathbb{N} \cup \{\infty\}, \min, +, \infty, 0 \rangle$ where $\infty + n = \infty = n + \infty$ and $\min\{n, \infty\} = n$
- Boolean semiring: $\langle \{\text{true}, \text{false}\}, \vee, \wedge, \text{false}, \text{true} \rangle$

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:

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

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

$$y + zx \leq z \implies yx^* \leq z$$

$$y + xz \leq z \implies x^*y \leq z$$

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

A Kleene algebra is $*$ -continuous iff

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

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

Kleene algebras – 2

Meaning of the axioms: a^* is the least x satisfying

$$1 + ax \leq x \qquad 1 + xa \leq x$$

In general, ba^* is the least x satisfying $b + xa \leq x$ and a^*b is the least x satisfying $b + xa \leq x$.

a^* is the least reflexive transitive element containing a , that is, the least x such that

$$1 \leq x \qquad a \leq x \qquad xx = x$$

Kleene algebras – 3

Proposition 1

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

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

$$\begin{aligned} x^0 + x \sum_{n \geq 0} x^n + \sum_{n \geq 0} x^n &= x^0 + \sum_{n \geq 0} x^{n+1} + \sum_{n \geq 0} x^n \\ &= \sum_{n \geq 0} x^n + \sum_{n \geq 0} x^n = \sum_{n \geq 0} x^n \end{aligned}$$

□

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:

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

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 $X \in \mathbf{KA}$ and $v : \Sigma \rightarrow X$.

Every $\langle X, v \rangle$ extends to an interpretation $\llbracket - \rrbracket_v : \mathbb{E}(\Sigma) \rightarrow X$ (homomorphism).

An equation $e \approx f$ is valid in KA iff $\llbracket e \rrbracket_v = \llbracket f \rrbracket_v$ for all $\langle X, v \rangle$.

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

Regular expressions – 2

Definition 5

The (canonical) language interpretation is $\llbracket - \rrbracket : \mathbb{E}(\Sigma) \rightarrow 2^{\Sigma^*}$ such that

$$\llbracket a \rrbracket = \{a\} \quad \llbracket 0 \rrbracket = \emptyset \quad \llbracket 1 \rrbracket = \{\epsilon\}$$

$$\llbracket e + f \rrbracket = \llbracket e \rrbracket \cup \llbracket f \rrbracket \quad \llbracket e \cdot f \rrbracket = \llbracket e \rrbracket \cdot \llbracket f \rrbracket \quad \llbracket e^* \rrbracket = \bigcup_{n \geq 0} \llbracket e \rrbracket^n = \llbracket e \rrbracket^*$$

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

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)

$\text{KA} \models e \approx f \text{ iff } \llbracket e \rrbracket = \llbracket f \rrbracket.$

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

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

Kleene algebras with tests – 1

Definition 6

A Kleene algebra with tests 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 $- : B \rightarrow B$ (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): $\langle 2^{Tr}, 2^{\text{States}}, \cup, \diamond, *, -, \emptyset, \text{States} \rangle$ 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:

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

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

We define:

$$\text{if } b \text{ then } e \text{ else } f := be + \bar{b}f \quad \text{while } b \text{ do } e := (be)^*\bar{b}$$

Regular expressions with tests – 2

Definition 8

A KAT model is $\langle X, v \rangle$ where $X \in \text{KAT}$ and $v : \Sigma \cup \Pi \rightarrow X$ such that $v(p) \in B$ for all $p \in \Pi$.

Every $\langle X, v \rangle$ extends to an interpretation $\llbracket - \rrbracket_v : \mathbb{E} \rightarrow X$ (homomorphism).

Validity: $\text{KAT} \models e \approx f$ iff $\llbracket e \rrbracket_v = \llbracket f \rrbracket_v$ 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 **if** b **then** e **else** f and **while** b **do** e induced by any $\langle X, v \rangle$ coincides with the relational and trace semantics of programs as defined in Part I of the course.

Regular expressions with tests – 3

We assume that Π is finite and comes with a fixed ordering: $p_1, \dots, p_n$.

Definition 9

An atom over Π is a sequence $r_1 \dots r_n$ where $r_i \in \{p_i, \bar{p}_i\}$. 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

$$S_1 a_1 S_2 \dots a_{n-1} S_n$$

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

We write $r_1 \dots r_n \models p_i$ iff $r_i = p_i$.

Regular expressions with tests – 4

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

Definition 10

The (canonical) language interpretation is $\llbracket - \rrbracket : \mathbb{E} \rightarrow 2^{GS}$ such that

$$\llbracket p \rrbracket = \{S \mid S \models p\} \quad \llbracket 0 \rrbracket = \emptyset \quad \llbracket 1 \rrbracket = A \quad \llbracket \bar{b} \rrbracket = A \setminus \llbracket b \rrbracket$$

$$\llbracket a \rrbracket = \{SaT \mid S, T \in A\}$$

$$\llbracket e + f \rrbracket = \llbracket e \rrbracket \cup \llbracket f \rrbracket \quad \llbracket e \cdot f \rrbracket = \llbracket e \rrbracket \diamond \llbracket f \rrbracket \quad \llbracket e^* \rrbracket = \bigcup_{n \geq 0} \llbracket e \rrbracket^n = \llbracket e \rrbracket^*$$

A guarded language $L \subseteq GS$ is regular iff there is $e \in \mathbb{E}$ such that $L = \llbracket e \rrbracket$.

KAT completeness

Theorem 2

The following are equivalent:

- 1 $\text{KAT} \models e \approx f$
- 2 $\text{KAT}^* \models e \approx f$
- 3 $\text{rKAT} \models e \approx f$
- 4 $\llbracket e \rrbracket = \llbracket f \rrbracket$

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

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

The function cay is injective. We can prove by induction on e that $\llbracket e \rrbracket_{\langle X, v \rangle} = \text{cay}(\llbracket e \rrbracket)$ for X the rKAT of binary relations on GS and $v(x) = \text{cay}(\llbracket x \rrbracket)$ for $x \in \Sigma \cup \Pi$.

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

Kleene algebra with antidomain – 1

Definition 11

A Kleene algebra with antidomain is $\langle X, +, \cdot, *, {}^\perp, 0, 1 \rangle$ where $\langle X, +, \cdot, *, 0, 1 \rangle$ is a Kleene algebra and

$${}^\perp : X \rightarrow X$$

such that $(x^\top =_{\text{def}} x^{\perp\perp})$

$$x^\perp \cdot x = 0 \qquad (x \cdot y)^\perp \leq (x \cdot y^\top)^\perp \qquad x^\perp + x^\top = 1$$

Intuition:

$x^\perp$ is a test of ‘program x does not terminate’ ($x^\top$ is a test of ‘ x does terminate’).

Kleene algebra with antidomain – 2

Examples

- KA of binary relations over S where

$$R^\perp = \{\langle s, s \rangle \mid \neg \exists t Rst\}$$

- KA of sets of traces over states S and actions Σ (i.e. sequences $s_1 a_1 s_2 \dots a_{n-1} s_n$ for $s_i \in S$ and $a_i \in \Sigma$), where

$$P^\perp = \{s \mid \neg \exists s_1 a_1 s_2 \dots a_{n-1} s_n \in P \text{ such that } s_1 = s\}$$

- KA of guarded languages over some Σ and Π such that

$$L^\perp = \{S \mid \neg \exists S_1 a_1 S_2 a_2 \dots a_{n-1} S_n \in L \text{ such that } S_1 = S\}$$

Kleene algebra with antidomain – 3

Let $X^\perp = \{x^\perp \mid x \in X\}$.

Proposition 4

The following hold in all KA with antidomain:

- 1 $0, 1 \in X^\perp$, which is closed under $+$ and $\cdot$.
- 2 $\langle X^\perp, +, \cdot, ^\perp, 0, 1 \rangle$ is a Boolean algebra
- 3 $x^\top \cdot x = x$
- 4 $(x + y)^\top = x^\top + y^\top$

Note: Not every KA can be extended with $^\perp$. E.g. $X = \{0, x, 1\}$ where $x \leq 1$ and $xx = 0$.

Proposition 5

$\langle X, X^\perp, +, \cdot, *, -, 0, 1 \rangle$, where $-$ is the restriction of $^\perp$ to $X^\perp$, is a KAT.

Definition 12

$$\langle x \rangle y =_{def} (x \cdot y)^\top \qquad [x]y =_{def} (x \cdot y^\perp)^\perp$$

Example

In an aKA of binary relations over S (for $P \subseteq 1_S$):

- $\langle R \rangle P = (R \circ P)^\top = \{ \langle s, s \rangle \mid \exists t (\langle s, t \rangle \in R \ \& \ \langle t, t \rangle \in P) \}$
- $[R]P = (R \circ P^\perp)^\perp = \{ \langle s, s \rangle \mid \forall t (\langle s, t \rangle \in R \implies \langle t, t \rangle \in P) \}$

$\text{KA}^\perp$ and PDL – 2

Let p, q etc. denote elements of $X^\perp$. We write $p \wedge q$ instead of pq and $p \vee q$ instead of $p + q$.

Proposition 6

The ‘translations’ of PDL axioms are valid in $\text{KA}^\perp$:

$$\langle 0 \rangle p = 0 = \langle x \rangle 0 \quad \langle 1 \rangle p = p \quad \langle x \rangle (p \vee q) = \langle x \rangle p \vee \langle x \rangle q$$

$$\langle x + y \rangle p = \langle x \rangle p \vee \langle y \rangle p \quad \langle xy \rangle p = \langle x \rangle \langle y \rangle p \quad \langle p \rangle q = p \wedge q$$

$$p \vee \langle x \rangle \langle x^* \rangle p = \langle x^* \rangle p \quad (p \vee \langle x \rangle q) \leq q \implies \langle x^* \rangle p \leq q$$

Hence, if $p = q$ is derivable from these translations (‘theorem of PDL’), then $p = q$ is valid in $\text{KA}^\perp$ (*PDL soundness*).

If $p = q$ is not a theorem of PDL, then $p \neq q$ in a relational $\text{KA}^\perp$ – the finite canonical model (*relational PDL completeness*).

$KA^\perp$ completeness – 1

$KA^\perp$ -terms are built from $\Sigma = \{a_i \mid i \in \mathbb{N}\}$ using operators $0, 1$ (nullary), $^\perp, *$ (unary) and $\cdot, +$ (binary). Let Tm be the set of terms.

Theorem 3

For all $e, f \in Tm$: $KA^\perp \models e \approx f$ iff $rKA^\perp \models e \approx f$.

Proof (sketch). If $KA^\perp \not\models e \approx f$, then by (Sedlár, 2023), Thm. 5, $TC \not\models \pi(e) \approx \pi(f)$ in Hollenberg's (1998) Test Calculus TC for PDL programs $\pi(e)$ and $\pi(f)$ obtained from e and f by re-numbering a_i to a_{2i} and defining $\pi(d^\perp) = [\pi(d)]^\perp$? (the translation function π commutes with $+, \cdot, *$ and $\pi(1) = \top$?, $\pi(0) = \perp$?). By (Hollenberg, 1998), Thm. 11, there is a PDL-model $\mathfrak{M}$ such that $R_{\pi(e)}^\mathfrak{M} \neq R_{\pi(f)}^\mathfrak{M}$. We can define a valuation $v : Tm \rightarrow \text{Rel}(\mathfrak{M})$ such that $v(e) = R_{\pi(e)}^\mathfrak{M}$ and $v(f) = R_{\pi(f)}^\mathfrak{M}$. Hence, $rKA^\perp \not\models e \approx f$. $\square$

$\text{KA}^\perp$ completeness – 2

Let $\text{tKA}^\perp$ be the class of *trace* $\text{KA}^\perp$'s over Σ .

Theorem 4

For all $e, f \in Tm$: $\text{KA}^\perp \models e \approx f$ iff $\text{tKA}^\perp \models e \approx f$.

Proof (sketch). By the previous theorem, if $\text{KA}^\perp \not\models e \approx f$, then there is $\text{Rel}(S) \in \text{rKA}^\perp$ of binary relations over S and a valuation $v : Tm \rightarrow \text{Rel}(S)$ such that $v(e) \neq v(f)$. We define $w : Tm \rightarrow \text{Tra}(S, \Sigma)$ where $w(a) = \{\text{sat} \mid \langle s, t \rangle \in v(a)\}$.

Let $w' : Tm \rightarrow \text{Rel}(S)$ where $w'(e) = \{\langle s, t \rangle \mid s \cdots t \in w(e)\}$ ('relational projection' of w). We have $w'(d) = v(d)$ for all $d \in Tm$, and so $\text{tKA}^\perp \not\models e \approx f$. □

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 $\text{KA} \models e \approx f$ iff $\text{KA}^* \models e \approx f$ iff $\text{rKA} \models e \approx f$. (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 $X \in \text{KAT}^*$:

$$\llbracket efg \rrbracket_v = \sum_{w \in \llbracket f \rrbracket} \llbracket ewg \rrbracket_v$$

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

- 8 Finish the proof of Proposition 6.

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).
- KA with antidomain is studied in (Desharnais and Struth, 2011), for example.
- Valid equations between PDL-programs are axiomatised in (Hollenberg, 1998). This result is used to establish the complexity of deciding validity of $\text{KA}^\perp$ equations in (Sedlár, 2023).

References

- Jules Desharnais and Georg Struth. Internal axioms for domain semirings. *Science of Computer Programming*, 76(3):181–203, 2011. Special issue on the Mathematics of Program Construction (MPC 2008).
- Marco Hollenberg. Equational axioms of test algebra. In M. Nielsen and W. Thomas, editors, *International Workshop on Computer Science Logic. CSL 1997*, pages 295–310, Berlin, Heidelberg, 1998. Springer.
- 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 Transactions on Programming Languages and Systems*, 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.
- Igor Sedlár. On the complexity of Kleene algebra with domain. In R. Glück, L. Santocanale, and M. Winter, editors, *Relational and Algebraic Methods in Computer Science (RAMiCS 2023)*, number 13896 in Lecture Notes in Computer Science, pages 208–223, Cham, 2023. Springer.