On the Complexity of Kleene Algebra With Domain

Igor Sedlár

Institute of Computer Science of the Czech Academy of Sciences

Prague, The Czech Republic

Czech Academy of Sciences

RAMiCS 2023
Augsburg, 3-6 April 2023

Introduction

- Kleene algebra with tests (Kozen, 1997): a two-sorted algebraic framework for reasoning about imperative programs. ($Eq(\mathsf{KAT})$ is PSPACE-complete; $Eq(\mathsf{KAT}) = Eq(\mathsf{KAT}^*) = Eq(\mathsf{RKAT})$.)
- Kleene algebra with domain (Desharnais et al., 2006; Desharnais and Struth, 2011): a one-sorted alternative.
- KAD extends KA with a unary antidomain operator, generalizing the properties of

$$\sim R := \{(s, s) \mid \neg\exists t.(s, t) \in R\}$$

  (divergence; dynamic negation of Groenendijk and Stokhof (1991))
- KAD is more expressive that KAT (Struth, 2016), but what about its complexity? What about KAD vs. KAD* vs. RKAD?

Contribution

- We show that the eq. theory of KAD is EXPTIME-complete
- Proof strategy: mutual reductions between KAD and the eq. theory of Relational Test Algebras (Hollenberg, 1997)
- Our proof also shows that $Eq(\mathsf{KAD}) = Eq(\mathsf{KAD}^*) = Eq(\mathsf{RKAD})$.

Outline:

$$\mathsf{KAD} \dashrightarrow \mathsf{RTA} \dashrightarrow (\mathsf{KAD} \overset{\hookleftarrow}{\hookrightarrow} \mathsf{RTA}) \dashrightarrow \text{Discussion}$$

Kleene algebra with domain

Kleene algebra with domain

Definition 1

A Kleene algebra with domain is

$$\mathcal{A} = (A, \cdot, +, {}^*, \mathsf{a}, 1, 0)$$

such that $(A, \cdot, +, {}^*, 1, 0)$ *is a Kleene algebra and (domain* $\mathsf{d} = \mathsf{a}^2$*)*

$$\mathsf{a}(x) \cdot x = 0 \tag{1}$$

$$\mathsf{a}(x \cdot y) \leq \mathsf{a}(x \cdot \mathsf{d}(y)) \tag{2}$$

$$\mathsf{d}(x) + \mathsf{a}(x) = 1 \tag{3}$$

*A Kleene algebra with domain is *-continuous iff its underlying Kleene algebra is *-continuous (i.e.* $xy^*z = \sum_{n\geq 0} xy^n z$*).*

Kleene algebra with domain – Examples

Example

Relational KAD: A relational Kleene algebra (A a set of binary relations, $\cdot$ composition, $+$ union, * reflexive transitive closure, 1 identity relation, $0 = \emptyset$) with $\sim$:

$$\sim R = \{(s,s) \mid \neg \exists t.(s,t) \in R\}$$

Note that $\sim\sim R = \{(s,s) \mid \exists t.(s,t) \in R\}$.

Example

Regular-language KAD: A Kleene algebra of regular languages over a finite alphabet Σ where

$$\mathsf{a}(L) = \begin{cases} \{\epsilon\} & \text{if } L = \emptyset \\ \emptyset & \text{otherwise.} \end{cases}$$

Kleene algebra with domain – Some facts

Proposition 1

The following hold in each Kleene algebra with domain, for all x, y, z:

1. $\mathsf{d}(x) \leq 1$ *(domain elements are subidentities)*
2. $\mathsf{d}(x)\mathsf{a}(x) = 0$ *(law of noncontradiction)*
3. $\mathsf{d}(x)x = x$ *(left invariant)*
4. $\mathsf{d}(x\mathsf{d}(y)) = \mathsf{d}(xy)$ *(locality)*
5. $\mathsf{d}(x + y) = \mathsf{d}(x) + \mathsf{d}(y)$ *(additivity)*
6. $\mathsf{d}(x)\mathsf{d}(y) = \mathsf{d}(\mathsf{d}(x)\mathsf{d}(y))$ (d-*multiplication)*

$\vdots$

Kleene algebra with domain – Some facts

Proposition 1

$\vdots$

7. $\mathsf{d}(x) + \mathsf{d}(y) = \mathsf{d}(\mathsf{d}(x) + \mathsf{d}(y))$ *(d-addition)*
8. $\mathsf{d}(1) = 1$ *and* $\mathsf{d}(0) = 0$ *(seriality and normality)*
9. $\mathsf{d}(x)\mathsf{d}(y) = \mathsf{d}(y)\mathsf{d}(x)$ *(domain elements are commutative)*
10. $\mathsf{d}(x)\mathsf{d}(x) = \mathsf{d}(x)$ *(domain elements are idempotent)*
11. $\mathsf{a}(x) = \mathsf{d}(\mathsf{a}(x))$ *and* $\mathsf{d}(x) = \mathsf{d}(\mathsf{d}(x))$ *(triple negation)*
12. $x \leq \mathsf{d}(y)x$ *iff* $\mathsf{d}(x) \leq \mathsf{d}(y)$ *(least left preserver)*

Kleene algebra with domain and KAT

For all $X \subseteq A$: $\mathsf{d}(X) = \{\mathsf{d}(x) \mid x \in X\}$.

Lemma 1

If $\mathcal{A} \in \mathrm{KAD}$*, then* $\mathsf{d}(\mathcal{A}) \in \mathrm{Sub}(\mathcal{A}) \cap \mathrm{BA}$*, where*

$$\mathsf{d}(\mathcal{A}) = (\mathsf{d}(A), \cdot, +, \mathsf{a}, 1, 0) .$$

It follows that $(A, \mathsf{d}(\mathcal{A}), \cdot, +, {}^*, \mathsf{a}, 1, 0) \in \mathrm{KAT}$.

However, not every KA extends to a KAD.

Kleene algebra with domain and PDL

Let $\langle x \rangle y := \mathsf{d}(xy)$. In RKAD, if $P \in 2^{S \times S}$ and $B \subseteq \mathrm{id}_S$:

$$
\begin{aligned}
\langle P \rangle B &= \mathsf{d}(P \circ B) \\
&= \{(s,s) \mid \exists t, u.(s,t) \in P \;\;\&\;\; (t,u) \in B\} \\
&= \{(s,s) \mid \exists t.(s,t) \in P \;\;\&\;\; (t,t) \in B\}
\end{aligned}
$$

Kleene algebra with domain and PDL

Lemma 2

The following hold in all Kleene algebras with domain, for all $x, y \in A$ and all $d, e \in \mathsf{d}(A)$:

1. $\langle x \rangle 0 = 0$ *and* $\langle 1 \rangle d = d$
2. $\langle x \rangle (d + e) = \langle x \rangle d + \langle x \rangle e$
3. $\langle x + y \rangle d = \langle x \rangle d + \langle y \rangle e$
4. $\langle xy \rangle d = \langle x \rangle \langle y \rangle d$
5. $\langle d \rangle e = de$
6. $\langle x^* \rangle d = d + \langle x \rangle \langle x^* \rangle d$
7. $d + \langle x \rangle e \leq e \rightarrow \langle x^* \rangle d \leq e$

Kleene algebra with domain – The equational theory

The set of KAD-terms Tm is defined using a countable set vrP of program variables as follows:

$$Tm \quad p, q := \mathtt{p}_n \mid 1 \mid 0 \mid p \cdot q \mid p + q \mid p^* \mid \mathsf{a}(p)$$

Equational theory: KAD $\models p \approx q$ iff $v(p) = v(q)$ for all momomorphisms $v : Tm \to \mathcal{A}$ where $\mathcal{A} \in$ KAD. (Notation: $p \approx q \in Eq(\text{KAD})$.)

$Eq(\text{KAD}^*)$ and $Eq(\text{RKAD})$ are defined as expected.

Relational test algebra

Relational test algebra (Hollenberg, 1997)

Definition 2

A relational test algebra is a structure of the form

$$\mathcal{T} = (\mathcal{K}, \mathcal{B}, \langle\,\rangle, ?)$$

where, for some $S \neq \emptyset$,

- $\mathcal{K} = (2^{S\times S}, \circ, \cup, {}^*, 1_S, \emptyset)$ *is the full relational Kleene algebra over S;*
- $\mathcal{B} = (2^S, \cap, \cup, {}^-, S, \emptyset)$ *is the Boolean algebra of subsets of S;*
- $\langle\rangle : \mathcal{K} \times \mathcal{B} \to \mathcal{B}$ *such that* $\langle R\rangle X = \{s \mid \exists t.(s,t) \in R \;\;\&\;\; t \in X\}$*;*
- $? : \mathcal{B} \to \mathcal{K}$ *such that* $X? = \{(s,s) \mid s \in X\}$*.*

Relational test algebra and KAD

For each $\mathcal{T}$, we have $\mathcal{T}^{\sim} \in \mathsf{RKAD}$ where $\mathcal{T}^{\sim} = (\mathcal{K}, \sim)$. Note that

$$\begin{aligned}
{\sim}R &= \{(s,s) \mid \neg\exists t.(s,t) \in R\}\\
&= \{(s,s) \mid \neg\exists t.(s,t) \in R \;\;\&\;\; t \in S\}\\
&= \{(s,s) \mid s \in \overline{\langle R\rangle S}\}\\
&= (\overline{\langle R\rangle S})?\,.
\end{aligned}$$

Relational test algebra – Program-equational theory

The sets of programs Pr and formulas Fm are defined by mutual induction as follows (using the sets of program variables $\mathtt{P}$ and Boolean variables $\mathtt{B}$):

$$
\begin{array}{ll}
Pr & \alpha, \beta := \mathtt{p}_n \mid 1 \mid 0 \mid \alpha ; \beta \mid \alpha \cup \beta \mid \alpha^* \mid \varphi ? \\
Fm & \varphi, \psi := \mathtt{b}_n \mid \bot \mid \neg\varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \langle\alpha\rangle\varphi \, .
\end{array}
$$

A program α is even iff $\mathtt{p}_n$ occurs in α only if n is even. We define $[\alpha]\varphi := \neg\langle\alpha\rangle\neg\varphi$.

Program-equational theory: the set of valid[1] equations of the form $\alpha \approx \beta$.

Hollenberg (1997) provides a proof system TC such that

$$TC \vdash \alpha \approx \beta \iff \mathsf{RTA} \models \alpha \approx \beta \, . \tag{4}$$

[1] $v(\alpha) = v(\beta)$ for all momomorphisms v from $Pr \cup Fm \to \mathcal{T}$.

Relational test algebra – Program-equational theory

Theorem 1

The following hold:

1. RTA $\models \alpha \approx \beta$ *iff* PDL $\models \varphi(\alpha, \beta)$.
2. PDL $\models \varphi$ *iff* RTA $\models (\varphi?) \approx 1$.
3. *The program eq. theory of* RTA *is EXPTIME-complete.*

Relational test algebra – The test calculus

Definition 3

TC *extends the axiomatizations of* KA *(Kozen, 1994) and* BA *with:*

- *test algebra axioms of (Trnková and Reiterman, 1987) (minus separability)*

(T1) $\langle \mathrm{p} \rangle \bot = \bot$

(T2) $\langle \mathrm{p} \rangle (\mathrm{b} \vee \mathrm{c}) = \langle \mathrm{p} \rangle \mathrm{b} \vee \langle \mathrm{p} \rangle \mathrm{c}$

(T3) $\langle 0 \rangle \mathrm{b} = \bot$

(T4) $\langle 1 \rangle \mathrm{b} = \mathrm{b}$

(T5) $\langle \mathrm{p} \cup \mathrm{q} \rangle \mathrm{b} = \langle \mathrm{b} \rangle \mathrm{p} \vee \langle \mathrm{q} \rangle \mathrm{p}$

(T6) $\langle \mathrm{pq} \rangle \mathrm{b} = \langle \mathrm{p} \rangle \langle \mathrm{q} \rangle \mathrm{b}$

(T7) $\langle \mathrm{p}^* \rangle \mathrm{b} = \mathrm{b} \vee \langle \mathrm{p} \rangle \langle \mathrm{p}^* \rangle \mathrm{b}$

(T8) $\langle \mathrm{p}^* \rangle \mathrm{b} = \mathrm{b} \vee \langle \mathrm{p}^* \rangle (\neg \mathrm{b} \wedge \langle \mathrm{p} \rangle \mathrm{b})$

(T9) $\langle \mathrm{b}? \rangle \mathrm{c} = \mathrm{b} \wedge \mathrm{c}$

- *and additional program axioms:*

(K1) $\bot ? = 0$

(K2) $(\mathrm{b} \vee \mathrm{c})? = \mathrm{b}? \cup \mathrm{c}?$

(K3) $(\mathrm{b} \wedge \mathrm{c})? = \mathrm{b}?\mathrm{c}?$

(K4) $(\langle \mathrm{p} \rangle \top)?\mathrm{p} = \mathrm{p}$

The inference rules are (Kozen's quasi-equations for * and) the usual inference rules of equational logic and uniform (sort-respecting) substitution.

The embedding results

The main result

We prove that there are functions $\tau : Pr \cup Fm \to Tm$ and $\sigma : Tm \to Pr$ such that, for all even α, β and all even p, q:

1. RTA $\models \alpha \approx \beta$ iff KAD $\models \tau(\alpha) \approx \tau(\beta)$
   (iff KAD* $\models \tau(\alpha) \approx \tau(\beta)$ iff RKAD $\models \tau(\alpha) \approx \tau(\beta)$)
2. KAD $\models p \approx \tau\sigma(p)$
   (only if KAD* $\models p \approx \tau\sigma(p)$ and RKAD $\models p \approx \tau\sigma(p)$).
3. RTA $\models \sigma(p) \approx \sigma(q)$ iff KAD $\models p \approx q$
   (iff KAD* $\models p \approx q$ iff RKAD $\models p \approx q$).

The main result, first part

Definition 4

Let τ be the following function from $Pr \cup Fm \to Tm$:

$$\tau(\mathtt{p}_{2n}) = \mathtt{p}_{2n}$$
$$\tau(\mathtt{p}_{2n+1}) = \mathtt{p}_{1}$$
$$\tau(1) = 1$$
$$\tau(0) = 0$$
$$\tau(\alpha \cup \beta) = \tau(\alpha) + \tau(\beta)$$
$$\tau(\alpha ; \beta) = \tau(\alpha) \cdot \tau(\beta)$$
$$\tau(\alpha^*) = \tau(\alpha)^*$$

$$\tau(\mathsf{b}_n) = \mathsf{d}(\mathtt{p}_{2n+1})$$
$$\tau(\bot) = 0$$
$$\tau(\neg\varphi) = \mathsf{a}(\tau(\varphi))$$
$$\tau(\varphi \wedge \psi) = \tau(\varphi) \cdot \tau(\psi)$$
$$\tau(\varphi \vee \psi) = \tau(\varphi) + \tau(\psi)$$
$$\tau(\langle\alpha\rangle\varphi) = \mathsf{d}(\tau(\alpha) \cdot \tau(\varphi))$$
$$\tau(\varphi?) = \tau(\varphi)$$

For each $\varphi \in Fm$ there is $p \in Tm$ such that KAD $\models \tau(\varphi) \approx \mathsf{d}(p)$.

The main result, first part

A. If RTA $\not\models \alpha \approx \beta$, then $v(\alpha) \neq v(\beta)$ for some $\mathcal{T} \in$ RTA. Take $\mathcal{T}^{\sim}$ and define w as the unique hom. $Tm \to \mathcal{T}^{\sim}$ such that:

$$w(\mathrm{p}_{2n}) = v(\mathrm{p}_{2n}) \qquad w(\mathrm{p}_{2n+1}) = v(\mathrm{b}_n?)\,.$$

Claim 1. For all γ, φ: $v(\gamma) = w(\tau(\gamma))$ and $v(\varphi?) = w(\tau(\varphi))$

It follows that RKAD $\not\models \tau(\alpha) \approx \tau(\beta)$
($\implies$ KAD* $\not\models \tau(\alpha) \approx \tau(\beta) \implies$ KAD $\not\models \tau(\alpha) \approx \tau(\beta)$).

B. If RTA $\models \alpha \approx \beta$, then $TC \vdash \alpha \approx \beta$ by Hollenberg's theorem (4).

Claim 2. For all γ_1, γ_2, $TC \vdash \gamma_1 \approx \gamma_2$ only if KAD $\models \tau(\gamma_1) \approx \tau(\gamma_2)$

It follows that KAD $\models \tau(\alpha) \approx \tau(\beta)$
($\implies$ KAD* $\models \tau(\alpha) \approx \tau(\beta) \implies$ RKAD $\models \tau(\alpha) \approx \tau(\beta)$).

The main result, second part

Definition 5

Let $\sigma : Tm \to Pr$ *be defined as follows:*

$$\begin{aligned}
\sigma(\mathtt{p}_n) &= \mathtt{p}_n \\
\sigma(1) &= \top? \\
\sigma(0) &= \bot? \\
\sigma(pq) &= \sigma(p);\sigma(q) \\
\sigma(p+q) &= \sigma(p) \cup \sigma(q) \\
\sigma(p^*) &= \sigma(p)^* \\
\sigma(\mathsf{a}(p)) &= ([\sigma(p)]\bot)?
\end{aligned}$$

Lemma 3

For each even term p*,* KAD $\models p \approx \tau\sigma(p)$*.*

The main result, second part

Proof of Lemma 3, the interesting case:

$$
\begin{aligned}
\tau\sigma(\mathsf{a}(p)) &= \tau(([\sigma(p)]\bot)?) \\
&= \tau([\sigma(p)]\bot) \\
&= \tau(\neg\langle\sigma(p)\rangle\top) \\
&= \mathsf{a}(\tau(\langle\sigma(p)\rangle\top)) \\
&= \mathsf{ad}(\tau\sigma(p)\cdot\tau(\neg\bot)) \\
&\equiv \mathsf{a}(p\cdot\mathsf{a}(0)) \\
&\equiv \mathsf{a}(p).
\end{aligned}
$$

The main result, third part

$$\mathsf{RTA} \models \sigma(p) \approx \sigma(q) \text{ iff } (\mathsf{R})\mathsf{KAD}^{(*)} \models \tau\sigma(p) \approx \tau\sigma(q) \quad \text{(by first part)}$$

$$\text{iff } (\mathsf{R})\mathsf{KAD}^{(*)} \models p \approx q \quad \text{(by second part)}$$

In particular,

$$\mathsf{KAD} \models p \approx q \text{ iff } \mathsf{KAD}^{*} \models p \approx q$$

$$\text{iff } \mathsf{RKAD} \models p \approx q$$

Discussion

Discussion

Main results: (Neither is shocking, but good to know.)

1. $Eq(\mathsf{KAD})$ is EXPTIME-complete.
2. $Eq(\mathsf{KAD}) = Eq(\mathsf{KAD}^*) = Eq(\mathsf{RKAD})$.

Open problem: Identify a natural generalization of KAD with a PSPACE-complete eq. theory.

Thank you!

References I

Jules Desharnais, Bernhard Möller, and Georg Struth.
Kleene algebra with domain.
ACM Trans. Comput. Logic, 7(4):798–833, oct 2006.

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).

Jeroen Groenendijk and Martin Stokhof.
Dynamic predicate logic.
Linguistics and Philosophy, 14(1):39–100, 1991.

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. Springer, 1997.

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.

References II

Georg Struth.
On the expressive power of Kleene algebra with domain.
Information Processing Letters, 116(4):284–288, 2016.

Věra Trnková and Jan Reiterman.
Dynamic algebras with test.
Journal of Computer and System Sciences, 35(2):229 – 242, 1987.