One-sorted Program Algebras[1]

I. Sedlár and J.J. Wannenburg

Institute of Computer Science of the Czech Academy of Sciences

LATD
September 2022

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

[1] This work was carried out within the project *Supporting the internationalization of the Institute of Computer Science of the Czech Academy of Sciences* (no. CZ.02.2.69/0.0/0.0/18_053/0017594), funded by the Operational Programme Research, Development and Education of the Ministry of Education, Youth and Sports of the Czech Republic. The project is co-funded by the EU.

Kleene algebra

Definition

A Kleene algebra [Koz94] is a structure $\mathscr{K} = (K, \vee, \cdot, {}^*, 1, 0)$ such that

- $(K, \vee, \cdot, 1, 0)$ is an *idempotent semiring*, i.e.,
  - $(K, \cdot, 1)$ is a monoid,
  - $(K, \vee, 0)$ is an idempotent commutative monoid (hence, a join-semilattice),
  - $x(y \vee z) = xy \vee xz$, $(y \vee z)x = yx \vee zx$, and
  - $x0 = 0 = 0x$, and
- ${}^* : K \to K$ such that

$$1 \vee a \vee a^*a^* \leq a^* \qquad ax \leq x \Rightarrow a^*x \leq x \qquad xa \leq x \Rightarrow xa^* \leq x$$

Examples: Kleene algebras of regular languages, Kleene algebra of paths...

Examples

Example

The relational Kleene algebra over a set X is $\mathscr{R}(X) = (2^{X \times X}, \cup, \circ, {}^*, \mathrm{id}, \emptyset)$;

- $\circ$ denotes composition, and
- $R^* = \bigcup_{i \geq 0} R^i$, where $R^0 = \mathrm{id}$ and $R^{i+1} = R \circ R^i$.

Example

The tropical Kleene algebra is defined over $0 > -1 > -2 > \cdots > -\omega$, where

- $+$ is multiplication,
- 0 is the *multiplicative* unit, and
- $-\omega$ the $\vee$ unit.

Kleene algebra with tests

Definition

A Kleene algebra with tests [Koz97] is $\mathscr{B} = (K, B, \vee, \cdot, ^*, 1, 0, ^-)$ where

- $(K, \vee, \cdot, ^*, 1, 0)$ is a Kleene algebra
- $B \subseteq K$
- $(B, \vee, \cdot, ^-, 1, 0)$ is a Boolean algebra.

Prop. Every KA is a KAT, where the test subalgebra is $B = \{0, 1\}$.

Examples

Example

The relational KAT over a set X is $\mathscr{R}(X)$ together with the Boolean test subalgebra 2^{id}.

Prop. [KS97] The equational theory of KAT is identical with the equational theory of rKAT.

Example

The only possible test subalgebra of the tropical Kleene algebra is $\{-\omega, 0\}$.

Propositional while programs

$$\text{Tests} \quad \beta := \mathsf{b} \mid \bar{\beta} \mid \beta \wedge \beta \mid \beta \vee \beta$$

$$\text{Programs} \quad \pi := \textbf{skip} \mid \mathsf{p} \mid \pi;\pi \mid \textbf{if } \beta \textbf{ then } \pi \textbf{ else } \pi \mid \textbf{while } \beta \textbf{ do } \pi$$

In KAT:

$$\textbf{skip} := b \vee \overline{b}$$
$$\textbf{if } b \textbf{ then } p \textbf{ else } q := (bp) \vee (\overline{b}q)$$
$$\textbf{while } b \textbf{ do } p := (bp)^*\overline{b}$$

Partial correctness: $bp = bpc$.

Kleene algebra with domain

Definition

A Kleene algebra with domain [DS11] is $\mathscr{D} = (K, \vee, \cdot, ^*, 1, 0, d)$ where $d : K \to K$ such that:

$$x = d(x)x$$
$$d(xy) = d(xd(y))$$
$$d(x) \leq 1$$
$$d(0) = 0$$
$$d(x \vee y) = d(x) \vee d(y)$$

(Similarly codomain c with $x \leq xc(x)$ and $c(xy) = c(c(x)y)$.)

Prop. $(d(K), \vee, \cdot, 1, 0)$ and $(c(K), \vee, \cdot, 1, 0)$ are bounded distr. lattices.

Open Prob. When is $(d(K), \vee, \cdot, 1, 0)$ a Heyting algebra?

Example

Example

Extend a relational Kleene algebra with

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

Intuitively, $d(x)$ should be the least left preserver of x under 1:

$$\text{if } y \leq 1, \text{ then } x \leq yx \iff d(x) \leq y \tag{1}$$

The equational theory of domain semirings (delete * and the corresponding axioms from KAD) coincides with the equational theory of relation algebras in the signature $(\cup, \circ, \emptyset, \mathrm{id}, d)$ [McL20].

Open Prob. What about the full signature with *?

Kleene algebra with antidomain

Definition

A Kleene algebra with antidomain [DS11] is $\mathscr{A} = (K, \vee, \cdot, ^*, 1, 0, a)$ where $a : K \to K$ such that

$$a(x)x = 0$$
$$a(xy) = a(xa^2(y))$$
$$a^2(x) \vee a(x) = 1$$

A domain operation is then defined by $d(x) := a^2(x)$.

Prop. $(d(K), \vee, \cdot, 1, 0)$ is a Boolean algebra where $a(x)$ is the complement of $x \in d(K)$.

Thm. The domain subalgebra of a KAAD is the maximal Boolean subalgebra of the semiring of elements $x \leq 1$.

Kleene algebra with (anti)domain

Example

Take a relational Kleene algebra and define

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

then $a(a(R)) = d(R)$.

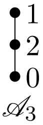
- The equational theory of relation algebras in the $(\circ, a, \emptyset, \mathrm{id})$ signature has been finitely axiomatized by equations [Hol97]
- The equational theory of KAAD is EXPTIME [MS06]

Thm. The equational theory of KAAD with $*$-*continuity* and *seperability* is EXPTIME-complete

Conj. The equational theory of KAAD coincides with that of rKAAD and the class above

Problem

However: **Prop.** Some finite KA cannot be extended with a domain operation.



$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	0

$*$	0	1	2
	1	1	1

The culprit is the locality axiom $d(xy) = d(xd(y))$.

Can one find a one-sorted alternative ALT to KAT that satisfies

1. ALT expands Kleene algebras by additional operations t and t'.
2. Every Kleene algebra extends to an ALT.
3. The test algebra $t(\mathscr{A})$ need not be the maximal Boolean subalgebra of elements $x \leq 1$.
4. The equational theory of KAT embeds into the equational theory of ALT.

One-sorted Kleene algebras with tests

Definition

A KAt is $\mathscr{K} = (K, \vee, \cdot, ^*, 1, 0, t, t')$ where $t, t' : K \to K$ such that

$$t(0) = 0 \tag{2}$$

$$t(1) = 1 \tag{3}$$

$$t(t(x) \vee t(y)) = t(x) \vee t(y) \tag{4}$$

$$t(t(x)t(y)) = t(x)\, t(y) \tag{5}$$

$$t(x)t(x) = t(x) \tag{6}$$

$$t(x) \leq 1 \tag{7}$$

$$1 \leq t'(t(x)) \vee t(x) \tag{8}$$

$$t'(t(x))\, t(x) \leq 0 \tag{9}$$

$$t'(t(x)) = t(t'(t(x))) \tag{10}$$

Examples

Example

Relational Kleene algebra with $t := d$ and $t' = a$.

Theorem 1

Every KAT $\mathscr{K} = (K, B, \vee, \cdot, ^*, 1, 0, ^-)$ *expands to a KAt* $\mathscr{K} = (K, \vee, \cdot, ^*, 1, 0, t, t')$, *i.e.,* $B = t(K)$.

In particular, we take

$$t(x) = \begin{cases} x & \text{if } x \in B \\ 1 & \text{otherwise.} \end{cases} \qquad t'(x) = \begin{cases} \bar{x} & \text{if } x \in B \\ x & \text{otherwise.} \end{cases}$$

Prop. Every Kleene algebra extends to a KAt, so KAt is a conservative extension of KAt.

Embedding result

Theorem 2

We show that equational theory of KAT embeds into the equational theory of ALT provided that

- *ALT expands Kleene algebras by additional operations t and t'.*
- *The test algebras $t(\mathscr{A})$ is a Boolean algebra for each ALT $\mathscr{A}$.*
- *Every KAT expands to an ALT.*

Proof sketch.
$Tr(\mathsf{p_n}) = \mathsf{x}_{2n}$, $Tr(\mathsf{b_n}) = t(\mathsf{x}_{2n+1})$, $Tr(\bar{b}) = t'(Tr(b))$;
Tr commutes with 1, 0, $\cdot$, $\vee$ and *.

If KAT $\not\models p \approx q$, which give rise to an expansion. Conversely, each ALT induces a Boolean algebra of tests, and hence a KAT. $\square$

Prop. The equational theory of KAT embeds into that of KAt.

So, KAt exhibits all the required properties (1-4).

Embedding result 2

Theorem 3

We show that equational theory of KAT embeds into the equational theory of ALT provided that

- *ALT expands Kleene algebras by additional operations t and t'.*
- *The test algebras $t(\mathscr{A})$ is a Boolean algebra for each ALT $\mathscr{A}$.*
- *Every relational KAT expands to an ALT.*

Proof sketch.

As before...

If KAT $\not\models p \approx q$, then $p \approx q$ fails in an rKAT, which gives rise to an expansion. Conversely, each ALT induces a Boolean algebra of tests, and hence a KAT. □

Prop. The equational theory of KAT embeds into that of KAD, but properties 2 and 3 fail.

strong KAt

Extending KAt with all of the following axioms retains properties (1-4)

$$t(x \vee y) = t(x) \vee t(y) \tag{11}$$

$$x \leq t(x)x \tag{12}$$

$$t(t(x)y) \leq t(x) \tag{13}$$

$$t(xy) \leq t(xt(y)) \tag{14}$$

(11) entails that t is monotonic; (12) says that $t(x)$ is a left preserver of x;
(13) entails that $t(x)$ is the *least* left preserver among tests;
(14) is called sublocality, and we can not add the reverse inequality.

One operation

Definition

In [AGS16] a 1KAT is $\mathscr{K} = (K, \vee, \cdot, ^*, 1, 0, a)$ where $a : K \to K$ such that

$$a^2(1) = 1 \tag{15}$$

$$a^2(a^2(x)\, a^2(y)) = a^2(y)\, a^2(x) \tag{16}$$

$$a(x)\, a^2(x) = 0 \tag{17}$$

$$a(x) \vee a(y) = a(a^2(x)\, a^2(y)) \tag{18}$$

- A 1KAT is a KAt where $t' = a$ and $t = a^2$
- 1KAT satisfies the conditions of Theorem 2
- 1KAT has properties 1-4

Residuated program algebras

Definition

A residuated KAt $\mathscr{P} = (K, \vee, \cdot, \to, \leftarrow, ^*, 1, 0, t)$ is a strong KAt (ignoring the t' axioms) that is extended with residuals for $\cdot$ satisfying

$$t(x \to y) \leq x \to xt(y) \tag{19}$$

$$1 \leq t(x) \vee (t(x) \to 0). \tag{20}$$

One can define $t'(x) := t(x \to 0)$, to obtain a KAt reduct.

Prop.: Every relational KAT expands to a residuated KAt, so the equational theory of KAT embeds into that of residuated KAt.

Another result: The substructural logic of partial correctness by Kozen and Tiuryn [KT03] embeds into *-continuous residuated KAt expanded by e such that $t(x) \leq y \iff x \leq e(y)$.

References I

Alasdair Armstrong, Victor B. F. Gomes, and Georg Struth.
Building program construction and verification tools from algebraic principles.
Formal Aspects of Computing, 28(2):265–293, April 2016.

Jules Desharnais and Georg Struth.
Internal axioms for domain semirings.
Science of Computer Programming, 76(3):181–203, March 2011.

Marco Hollenberg.
An Equational Axiomatization of Dynamic Negation and Relational Composition.
Journal of Logic, Language and Information, 6(4):381–401, October 1997.

D. Kozen.
A Completeness Theorem for Kleene Algebras and the Algebra of Regular Events.
Information and Computation, 110(2):366–390, May 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 Gerhard Goos, Juris Hartmanis, Jan Leeuwen, Dirk Dalen, and Marc Bezem, editors, *Computer Science Logic*, volume 1258, pages 244–259. Springer Berlin Heidelberg, Berlin, Heidelberg, 1997.

References II

Dexter Kozen and Jerzy Tiuryn.
Substructural logic and partial correctness.
ACM Transactions on Computational Logic, 4(3):355–378, July 2003.

Brett McLean.
Free Kleene algebras with domain.
Journal of Logical and Algebraic Methods in Programming, 117:100606, December 2020.

Bernhard Möller and Georg Struth.
Algebras of modal operators and partial correctness.
Theoretical Computer Science, 351(2):221–239, February 2006.