Embedding Kozen-Tiuryn Logic into Residuated One-sorted Kleene Algebra With Tests[1]

I. Sedlár and J.J. Wannenburg

Institute of Computer Science of the Czech Academy of Sciences

LOGICA
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

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

$\mathscr{K}$ is *-continuous iff $ab^*c = \bigvee_{n \geq 0} ab^nc$.

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 $R^{i+1} = R \circ R^i$.

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 $B = \{0, 1\}$.

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 to the equational theory of rKAT.

Propositional while programs

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

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

In KAT:

$$b \wedge c := bc \qquad b \vee c := b \vee c$$

$$p;q := pq$$

$$\textbf{skip} := b \vee \bar{b}$$

$$\textbf{if } b \textbf{ then } p \textbf{ else } q := (bp) \vee (\bar{b}q)$$

$$\textbf{while } b \textbf{ do } p := (bp)^*\bar{b}$$

Non-termination: $p = 0$

Partial correctness: $\{b\}p\{c\} \iff bp = bpc$

Kozen-Tiuryn Logic

In [KT03] Kozen and Tiuryn introduces a logic (see next 2 slides) which represents partial correctness by a formula, instead of an equation in KAT. They argue that this has certain advantages, e.g., it facilitates a better distinction between local and global properties.

Kozen-Tiuryn Logic

Definition

Let $\mathsf{B} = \{\mathsf{b}_i \mid i \in \omega\}$ be the set of test variables and let $\mathsf{P} = \{\mathsf{p}_i \mid i \in \omega\}$ be the set of program variables.
We define the following sorts of syntactic objects:

tests	$b, c := \mathsf{b}_i \mid 0 \mid b \Rightarrow c$
programs	$p, q := \mathsf{p}_i \mid b \mid p \oplus q \mid p \otimes q \mid p^+$
formulas	$f, g := b \mid p \Rightarrow f$
environments	$\Gamma, \Delta := \epsilon \mid \Gamma, p \mid \Gamma, f$
sequents	$\Gamma \vdash f$

We define $1 := 0 \Rightarrow 0$, $\neg b := b \Rightarrow 0$ and $p^* := 1 \oplus p^+$.
The logic S is defined in [KT03] to be the set of sequents provable in the following proof system:

(Id) $b \vdash b$

(TC) $$\frac{\Gamma, b, \Delta \vdash f \qquad \Gamma, \overline{b}, \Delta \vdash f}{\Gamma, \Delta \vdash f}$$

(R⇒) $$\frac{\Gamma, p \vdash f}{\Gamma \vdash p \Rightarrow f}$$

(I⊗) $$\frac{\Gamma, p, q, \Delta \vdash f}{\Gamma, p \otimes q, \Delta \vdash f}$$

(I⊕) $$\frac{\Gamma, p, \Delta \vdash f \qquad \Gamma, q, \Delta \vdash f}{\Gamma, p \oplus q, \Delta \vdash f}$$

(I$^+$) $$\frac{g, p \vdash f \qquad g, p \vdash g}{g, p^+ \vdash f}$$

(E$^+$) $$\frac{\Gamma, p^+, \Delta \vdash f}{\Gamma, p, \Delta \vdash f}$$

(CC$^+$) $$\frac{\Gamma, p^+, \Delta \vdash f}{\Gamma, p^+, p^+, \Delta \vdash f}$$

(I0) $\Gamma, 0, \Delta \vdash f$

(cut) $$\frac{\Gamma \vdash g \qquad \Gamma, g, \Delta \vdash f}{\Gamma, \Delta \vdash f}$$

(I⇒) $$\frac{\Gamma, p, f, \Delta \vdash g}{\Gamma, p \Rightarrow f, p, \Delta \vdash g}$$

(E⊗) $$\frac{\Gamma, p \otimes q, \Delta \vdash f}{\Gamma, p, q, \Delta \vdash f}$$

(E$\oplus_1$) $$\frac{\Gamma, p \oplus q, \Delta \vdash f}{\Gamma, p, \Delta \vdash f}$$

(E$\oplus_2$) $$\frac{\Gamma, p \oplus q, \Delta \vdash f}{\Gamma, q, \Delta \vdash f}$$

(Wf) $$\frac{\Gamma, \Delta \vdash g}{\Gamma, f, \Delta \vdash g}$$

(Wp) $$\frac{\Gamma \vdash f}{p, \Gamma \vdash f}$$

Binary relation semantics

Definition

A Kozen–Tiuryn model is a pair $M = (W, V)$, where W is a non-empty set and $V : \mathsf{B} \cup \mathsf{P} \to \mathscr{R}(W)$ such that $V(\mathsf{b}) \subseteq \mathrm{id}_W$ for all $\mathsf{b} \in \mathsf{B}$.
We define the M-interpretation function $[\,]_M : Ex_{\mathsf{S}} \to \mathscr{R}(W)$ as follows:

- $[\mathsf{b}]_M = V(\mathsf{b})$, $\quad [\mathsf{p}]_M = V(\mathsf{p})$, $\quad [0]_M = \emptyset$
- $[b \Rightarrow c]_M = \{(s,s) \mid (s,s) \notin [b]_M$ or $(s,s) \in [c]_M\}$
- $[p \oplus q]_M = [p]_M \cup [q]_M$
- $[p \otimes q]_M = [p]_M \circ [q]_M$
- $[p^+]_M = [p]_M^+$
- $[p \Rightarrow f]_M = \{(s,s) \mid \forall t.(s,t) \in [p]_M \implies (t,t) \in [f]_M\}$
- $[\epsilon]_M = \mathrm{id}_W$
- $[\Gamma, \Delta]_M = [\Gamma]_M \circ [\Delta]_M$

(Here $^+$ denotes transitive closure and $\circ$ denotes relational composition.)

Definition

A sequent $\Gamma \vdash f$ is valid in M iff,
for all $s, t \in W$, if $(s,t) \in [\![\Gamma]\!]_M$, then $(t,t) \in [\![f]\!]_M$.

Theorem 1

$\Gamma \vdash f$ is provable in S iff $\Gamma \vdash f$ is valid in every Kozen–Tiuryn model.

- Observe that $[\![f]\!]_M \subseteq \mathrm{id}_W$ for all formulas f
- If $(s,s) \in [\![f]\!]_M$, then we may say that formula f is true in s.
- Note that $[\![bp \Rightarrow c]\!]_M$ is the set of (s,s) such that, for all t, if $(s,s) \in [\![b]\!]_M$ and $(s,t) \in [\![p]\!]_M$, then $(t,t) \in [\![c]\!]_M$.
- Hence, $bp \Rightarrow c$ represents a partial correctness assertion: the formula is true in s iff b is true in s and p connects s with a state t only if c is true in t.

Questions

- How does S relate to mainstream substructural logic?
- Is there a one-sorted residuated structure into which we can interpret S?

Residuals

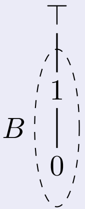
Definition

An idempotent semiring is residuated if it has two binary operation $\to$, $\hookrightarrow$ such that

$$xy \leq z \iff x \leq y \to z \iff y \leq x \hookrightarrow z. \qquad (1)$$

Note. One can not translate $p \Rightarrow b$ to $p \to b$, since $0 \to 0$ is maximal.

Example



$\to$	0	1	$\top$
0	$\top$	$\top$	$\top$
1	0	1	$\top$
$\top$	0	0	$\top$

$\cdot$	0	1	$\top$
0	0	0	0
1	0	1	$\top$
$\top$	0	$\top$	$\top$

$*$	0	1	$\top$
	1	1	$\top$

Let $R \subseteq S \times S$ and $B \subseteq \mathrm{id}_S$.

$$R \to B = \{(s,u) \mid \forall v.\,(u,v) \in R \implies (s,v) \in B\}$$
$$R \Rightarrow B = \{(u,u) \mid \forall v.\,(u,v) \in R \implies (v,v) \in B\}$$

Now consider the operations $c, e : 2^{S\times S} \to 2^{S\times S}$

$$c(R) = \{(u,u) \mid \exists s.\,(s,u) \in R\} \tag{2}$$
$$e(R) = \{(s,u) \mid (u,u) \in R\} \tag{3}$$

Note that c and e form a *Galois connection* in the sense that,

$$c(R) \subseteq Q \iff R \subseteq e(Q)\,. \tag{4}$$

Proposition 1

$$c(R \to e(B)) = R \Rightarrow B \tag{5}$$

Kleene algebra with codomain

The following one-sorted alternative to KAT is presented in [DS11].

Definition

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

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

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

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

Thm. The equational theory of KAT embeds into that of KAC.

Relational KAC

Example

Extend a relational Kleene algebra with

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

Thus creating a relational KAC.

The codomain operation $a(a(R)) = c(R)$, is then as expected

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

Residuated program algebras

Definition

An SKAT $\mathscr{P} = (K, \vee, \cdot, \to, \hookrightarrow {}^*, a, e, 1, 0)$ comprises

- a residuated Kleene algebra $(K, \vee, \cdot, \hookrightarrow, \to, {}^*, 1, 0)$,
- a Kleene algebra with codomain $(K, \vee, \cdot, {}^*, a, 1, 0)$, and
- a unary operation e on K that satisfies the following:

$$a(a(e(x))) \leq x \tag{6}$$

$$x \leq e(a(a(x))) \tag{7}$$

$$e(x) \leq e(x \vee y) \tag{8}$$

We define $c(x) := a(a(x))$. An SKAT is *-continuous (denoted SKAT*) iff its underlying Kleene algebra is *-continuous.

Prop.: The class of all SKATs is a variety.

Embedding result

Let Tm be the absolutely free SKAT-type algebra over $\{x_1, x_2, \dots\}$.

Definition

We define $Tr : Ex_{\mathsf{S}} \to Tm$ as follows:

- $Tr(\mathsf{p}_n) = \mathsf{x}_{2n}, \quad Tr(\mathsf{b}_n) = c(\mathsf{x}_{2n+1}), \quad Tr(0) = c(0), \quad Tr(\epsilon) = 1$
- $Tr(b \Rightarrow c) = c(Tr(b) \to e(Tr(c)))$
- $Tr(p \oplus q) = Tr(p) \vee Tr(q)$
- $Tr(p \otimes q) = Tr(p) \cdot Tr(q)$
- $Tr(p^+) = Tr(p) \cdot Tr(p)^*$
- $Tr(p \Rightarrow f) = c(Tr(p) \to e(Tr(f)))$
- $Tr(\Gamma, \Delta) = Tr(\Gamma) \cdot Tr(\Delta)$

Theorem 2

A sequent $\Gamma \vdash f$ is provable in S iff $c\big(Tr(\Gamma)\big) \leq Tr(f)$ belongs to the equational theory of *-continuous SKAT.

References I

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

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.

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