Kleene algebra with hypotheses

A. Doumane[1,2] D. Kuperberg[1] D. Pous[1] P. Pradic[1,2]

[1]CNRS,LIP,ENS Lyon
[2]Warsaw University

Fossacs, ETAPS, Prague
April 11th 2019

Kleene Algebra

Regular expressions

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

Intuition : $x^* = \bigcup_{i \in \mathbb{N}} x^i$.
$x \leq y$ shorthand for $x + y = y$

Kleene Algebra

Regular expressions

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

Intuition : $x^* = \bigcup_{i \in \mathbb{N}} x^i$.
$x \leq y$ shorthand for $x + y = y$

$(M, +, \cdot, *, 0, 1)$ is a Kleene algebra if:

Axioms of KA

$(M, +, \cdot, 0, 1)$ is an idempotent semiring

$$1 + xx^* \leq x^* \qquad xy \leq y \;\Rightarrow\; x^*y \leq y$$

$$1 + x^*x \leq x^* \qquad yx \leq y \;\Rightarrow\; yx^* \leq y$$

Some concrete Kleene algebras

Models of KA:

- Formal languages: $(\Sigma^*, \cup, \cdot, *, \emptyset, \{\epsilon\})$
- Regular languages: $(\mathrm{Reg}, \cup, \cdot, *, \emptyset, \{\epsilon\})$
- Relations on a set S: $(\mathcal{P}(S \times S), \cup, \circ, *, \emptyset, id)$
- Tropical algebra: $(\mathbb{R} \cup \{-\infty\}, \min, +, *, -\infty, 0)$

  interpret shortest path algorithm
- $n \times n$ matrices over a KA K: $(M_n(K), +, \cdot, *, 0, Id)$

Some concrete Kleene algebras

Models of KA:

- Formal languages: $(\Sigma^*, \cup, \cdot, *, \emptyset, \{\epsilon\})$
- Regular languages: $(\mathrm{Reg}, \cup, \cdot, *, \emptyset, \{\epsilon\})$
- Relations on a set S: $(\mathcal{P}(S \times S), \cup, \circ, *, \emptyset, id)$
- Tropical algebra: $(\mathbb{R} \cup \{-\infty\}, \min, +, *, -\infty, 0)$

  interpret shortest path algorithm
- $n \times n$ matrices over a KA K: $(M_n(K), +, \cdot, *, 0, Id)$

Theorem (Boffa '90+Krob '91, Kozen '94)

The model $(\mathrm{Reg}_, +, \cdot, *, \emptyset, \{\epsilon\})$ *of regular languages is complete:*

$$KA \vdash e \leq f \Leftrightarrow L(e) \subseteq L(f)$$

Consequence:

Equational theory of KA is decidable and PSPACE-complete.

KA for verification

Programs can be modeled by Relations on S: memory states.
$+$ is nondeterministic choice, $\cdot$ is sequential composition, $*$ is loop

KA for verification

Programs can be modeled by Relations on S: memory states.
$+$ is nondeterministic choice, $\cdot$ is sequential composition, $*$ is loop

Example:
$$\begin{array}{lcc} \text{Program 1} & \rightsquigarrow & (A+B)^* \\ \text{Program 2} & \rightsquigarrow & A^*; B^* \end{array}$$

KA for verification

Programs can be modeled by Relations on S: memory states.
$+$ is nondeterministic choice, $\cdot$ is sequential composition, $*$ is loop

Example:

$$\begin{array}{lcl} \text{Program 1} & \rightsquigarrow & (A+B)^* \\ \text{Program 2} & \rightsquigarrow & A^*; B^* \end{array}$$

Hypotheses are necessary to get interesting abstractions.

KA for verification

Programs can be modeled by Relations on S: memory states.
$+$ is nondeterministic choice, $\cdot$ is sequential composition, $*$ is loop

Example: Program 1 $\rightsquigarrow$ $(A+B)^*$
Program 2 $\rightsquigarrow$ $A^*; B^*$

Hypotheses are necessary to get interesting abstractions.

Example: A : x := 1
B : y := 2

KA for verification

Programs can be modeled by Relations on S: memory states.
$+$ is nondeterministic choice, $\cdot$ is sequential composition, $*$ is loop

Example:

$$\begin{array}{lcl} \text{Program 1} & \rightsquigarrow & (A+B)^* \\ \text{Program 2} & \rightsquigarrow & A^*; B^* \end{array}$$

Hypotheses are necessary to get interesting abstractions.

Example:

$$\begin{array}{l} A: \quad \mathsf{x} := 1 \\ B: \quad \mathsf{y} := 2 \\ B; A = A; B \end{array}$$

KA for verification

Programs can be modeled by Relations on S: memory states.
$+$ is nondeterministic choice, $\cdot$ is sequential composition, $*$ is loop

Example:

$$\begin{array}{lcc} \text{Program 1} & \rightsquigarrow & (A+B)^* \\ \text{Program 2} & \rightsquigarrow & A^*; B^* \end{array}$$

Hypotheses are necessary to get interesting abstractions.

Example:

$$\begin{array}{rl} A: & \mathsf{x} := 1 \\ B: & \mathsf{y} := 2 \\ & B; A = A; B \\ \Rightarrow & (A+B)^* = A^*; B^*. \end{array}$$

KA for verification

Programs can be modeled by Relations on S: memory states.
$+$ is nondeterministic choice, $\cdot$ is sequential composition, $*$ is loop

Example:

$$\begin{array}{lcc} \text{Program 1} & \rightsquigarrow & (A+B)^* \\ \text{Program 2} & \rightsquigarrow & A^*; B^* \end{array}$$

Hypotheses are necessary to get interesting abstractions.

Example:

$$\begin{array}{rl} A: & x := 1 \\ B: & y := 2 \\ & B; A = A; B \\ \Rightarrow & (A+B)^* = A^*; B^*. \end{array}$$

KA for verification

Programs can be modeled by Relations on S: memory states.
$+$ is nondeterministic choice, $\cdot$ is sequential composition, $*$ is loop

Example:

$$\begin{array}{lcc} \text{Program 1} & \rightsquigarrow & (A+B)^* \\ \text{Program 2} & \rightsquigarrow & A^*; B^* \end{array}$$

Hypotheses are necessary to get interesting abstractions.

Example:

$$\begin{array}{c} A: \quad \mathsf{x} := 1 \\ B: \quad \mathsf{y} := 2 \\ B; A = A; B \\ \Rightarrow \quad (A+B)^* = A^*; B^*. \end{array}$$

~~Equational theory of KA~~
Horn Theory of KA $\equiv$ equational theory of KA_H

Star continuity

Intended meaning of star: $x^* = \bigcup_{i \in \mathbb{N}} x^i$.

KA*: KA + this axiom:

Star continuity axiom

$$(\forall i \in \mathbb{N},\ xy^i z \leq t) \quad \Rightarrow \quad xy^* z \leq t$$

Star continuity

Intended meaning of star: $x^* = \bigcup_{i \in \mathbb{N}} x^i$.

KA*: KA + this axiom:

Star continuity axiom

$$(\forall i \in \mathbb{N},\ xy^i z \leq t) \quad \Rightarrow \quad xy^* z \leq t$$

Equational Theory: KA $\equiv$ KA* [Kozen '94]

Star continuity

Intended meaning of star: $x^* = \bigcup_{i \in \mathbb{N}} x^i$.

KA*: KA + this axiom:

Star continuity axiom

$$(\forall i \in \mathbb{N},\ xy^i z \leq t) \quad \Rightarrow \quad xy^* z \leq t$$

Equational Theory: KA $\equiv$ KA* [Kozen '94]
Horn Theory: KA$_H$ $\not\equiv$ KA$^*_H$ [Kozen '90], refutes Conway's conjecture

Star continuity

Intended meaning of star: $x^* = \bigcup_{i \in \mathbb{N}} x^i$.

KA*: KA + this axiom:

Star continuity axiom

$$(\forall i \in \mathbb{N},\ xy^i z \leq t) \quad \Rightarrow \quad xy^* z \leq t$$

Equational Theory: KA $\equiv$ KA* [Kozen '94]
Horn Theory: $KA_H \not\equiv KA^*_H$ [Kozen '90], refutes Conway's conjecture

Horn KA* algorithmic problem:
Input: set $H = \{e_i \leq f_i, i \in I\}$ of hypotheses, and target $e \leq f$
Output: Does $KA^*_H \models e \leq$ f hold ?

Research Program [Kozen, Cohen, Conway]
Complexity depending on restrictions on H?

Previous results

Notations for H: a, b: letters; u, v words; e, f expressions.

Decidable cases, if equations in H are of the form:

- $e = 0$ [Cohen 94]
- $a \leq 1$: models **tests** [Cohen 94]

$$\begin{bmatrix}1 & 0 & 0 & 0\\0 & 0 & 0 & 0\\0 & 0 & 1 & 0\\0 & 0 & 0 & 1\end{bmatrix}$$

- $1 = u$ or $a = u$, (under certain conditions),
  examples: $1 = aa \quad a = aa$ [Kozen+Mamouras 2014]

Previous results

Notations for H: a, b: letters; u, v words; e, f expressions.

Decidable cases, if equations in H are of the form:

- $e = 0$ [Cohen 94]
- $a \leq 1$: models **tests** [Cohen 94] $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
- $1 = u$ or $a = u$, (under certain conditions), examples: $1 = aa \quad a = aa$ [Kozen+Mamouras 2014]

Case $1 = \sum_i a_i$ left open by Cohen,
Useful for case analysis

Previous results

Notations for H: a, b: letters; u, v words; e, f expressions.

Decidable cases, if equations in H are of the form:

- $e = 0$ [Cohen 94]
- $a \leq 1$: models **tests** [Cohen 94] $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
- $1 = u$ or $a = u$, (under certain conditions), examples: $1 = aa \quad a = aa$ [Kozen+Mamouras 2014]

Case $1 = \sum_i a_i$ left open by Cohen,
Useful for case analysis

Undecidable cases (Cohen '94, Kozen 2002)

- $ab = ba$: Π^0_1-complete (KA: EXPSPACE-hard)
- $u = v$: Π^0_2-complete (KA: Σ^0_1-complete)
- $e \leq f$: Π^1_1-complete (KA: Σ^0_1-complete)

This paper

Our goal:

- Understand better the decidability frontier
- Stengthen Kozen's hardness results
- Solve Cohen's open problem $1 = \sum_i a_i$
- Study related cases $a \leq \sum_i a_i$ and $a \leq \sum_i u_i$

This paper

Our goal:

- Understand better the decidability frontier
- Stengthen Kozen's hardness results
- Solve Cohen's open problem $1 = \sum_i a_i$
- Study related cases $a \leq \sum_i a_i$ and $a \leq \sum_i u_i$

From now on, hypotheses are *simple*: $a \leq \sum_i u_i$

H-closure of languages

H-closure of a language L

$cl_H(L)$ is the smallest language such that

- $L \subseteq cl_H(L)$
- $\left(\forall i \in I,\ x u_i y \in cl_H(L)\right) \Rightarrow x a y \in cl_H(L)$

$a \leq \sum_{i \in I} u_i$ hypothese in H, x, y arbitrary words

Example: $L = \{ant, bat, cat, rat\}$, H :

$$e \leq t \quad (1)$$
$$p \leq n + a \quad (2)$$
$$a \leq b + c + r \quad (3)$$

Do we have $ape \in \mathrm{cl}_H(L)$?

H-closure of languages

H-closure of a language L

$cl_H(L)$ is the smallest language such that

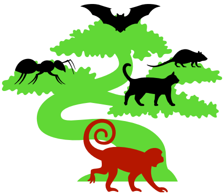
- $L \subseteq cl_H(L)$
- $\left(\forall i \in I,\ x u_i y \in cl_H(L)\right) \Rightarrow x a y \in cl_H(L)$

$a \leq \sum_{i \in I} u_i$ hypothese in H, $\quad x, y$ arbitrary words

Example: $L = \{ant, bat, cat, rat\}$, $\quad H$:

$$e \leq t \qquad (1)$$
$$p \leq n + a \qquad (2)$$
$$a \leq b + c + r \qquad (3)$$

Do we have $ape \in \mathrm{cl}_H(L)$?



$$\dfrac{\dfrac{ant \qquad \dfrac{bat \quad cat \quad rat}{aat}\,(3)}{apt}\,(2)}{ape}\,(1)$$

Relating closure and Kleene algebra

Theorem

For all hypotheses H, and expressions e, f:

$$\mathsf{KA}_H^* \models e \leq f \qquad \Leftrightarrow \qquad L(e) \subseteq \mathrm{cl}_H(L(f))$$

Is $cl_H(L)$ regular when L regular ?

Relating closure and Kleene algebra

Theorem

For all hypotheses H, and expressions e, f:

$$\mathsf{KA}^*_H \models e \leq f \qquad \Leftrightarrow \qquad L(e) \subseteq \mathrm{cl}_H(L(f))$$

Is $cl_H(L)$ regular when L regular ?

Hypotheses	Regularity	Decidability
$1 = \sum_i a_i$.	Yes (effective)	KA^*_H decidable for $1 = \sum_i a_i$. answers Cohen's problem

Relating closure and Kleene algebra

Theorem

For all hypotheses H, and expressions e, f:

$$\mathsf{KA}^*_H \models e \leq f \qquad \Leftrightarrow \qquad L(e) \subseteq \mathrm{cl}_H(L(f))$$

Is $cl_H(L)$ regular when L regular ?

Hypotheses	Regularity	Decidability
$1 = \sum_i a_i$.	Yes (effective)	KA^*_H decidable for $1 = \sum_i a_i$. answers Cohen's problem
$a \leq \sum_i a_i$	No	KA^*_H undecidable for $a \leq \sum_i a_i$.

Our results

Decidability of Cohen's hypotheses $1 = \sum_i a_i$

	$a \leq \sum b$	$a \leq \sum w$	$a \leq f$
$\mathsf{KA}_H \vdash u \leq f$	$\mathrm{EXPTIME-c}$	Σ^0_1−complete	Σ^0_1−complete
$\mathsf{KA}_H \vdash e \leq f$	Undecidable	Σ^0_1−complete	Σ^0_1−complete
$\mathsf{KA}^*_H \vdash u \leq f$	$\mathrm{EXPTIME-c}$	Σ^0_1−complete	Π^1_1−complete
$\mathsf{KA}^*_H \vdash e \leq f$	Π^0_1−complete	Π^0_2−complete	Π^1_1−complete

Ideas: Encode LBA, Turing machines

Recursion-theoretic arguments

Our results

Decidability of Cohen's hypotheses $1 = \sum_i a_i$

	$a \leq \sum b$	$a \leq \sum w$	$a \leq f$
$KA_H \vdash u \leq f$	$\mathrm{EXPTIME} - \mathrm{c}$	Σ_1^0−complete	Σ_1^0−complete
$KA_H \vdash e \leq f$	Undecidable	Σ_1^0−complete	Σ_1^0−complete
$KA_H^* \vdash u \leq f$	$\mathrm{EXPTIME} - \mathrm{c}$	Σ_1^0−complete	Π_1^1−complete
$KA_H^* \vdash e \leq f$	Π_1^0−complete	Π_2^0−complete	Π_1^1−complete

Ideas: Encode LBA, Turing machines
Recursion-theoretic arguments

Future work:

- Refine bounds
- Link with recent works
  e.g. Kuznetsov '19: The logic of action lattices is undecidable
- Coq implementations