On Tools for Completeness of Kleene Algebra with Hypotheses

Damien Pous
Jurriaan Rot
Jana Wagemaker
Radboud Universiteit Nijmegen
ENS Lyon

Overview

- Kleene algebra: axiomatisation of regular languages

Overview

- Kleene algebra: axiomatisation of regular languages
- Many variants and extensions:
  - Kleene algebra with tests (KAT)
  - NetKAT
  - Concurrent extensions (CKA, POCKA, CKAO, …)
  - …

Overview

- Kleene algebra: axiomatisation of regular languages
- Many variants and extensions:
  - Kleene algebra with tests (KAT)
  - NetKAT
  - Concurrent extensions (CKA, POCKA, CKAO, …)
  - …
- Completeness: typically by reduction to (concurrent) Kleene algebra

Overview

- Kleene algebra: axiomatisation of regular languages
- Many variants and extensions:
  - Kleene algebra with tests (KAT)
  - NetKAT
  - Concurrent extensions (CKA, POCKA, CKAO, . . .)
  - . . .
- Completeness: typically by reduction to (concurrent) Kleene algebra
- Unifying foundation: Kleene algebra with Hypotheses (Cohen, Kozen, Mamouras, Doumane et al, Kappé et al, . . .)

Overview

- Kleene algebra: axiomatisation of regular languages
- Many variants and extensions:
  - Kleene algebra with tests (KAT)
  - NetKAT
  - Concurrent extensions (CKA, POCKA, CKAO, ...)
  - ...
- Completeness: typically by reduction to (concurrent) Kleene algebra

- Unifying foundation: Kleene algebra with Hypotheses (Cohen, Kozen, Mamouras, Doumane et al, Kappé et al, ...)
- This paper: collecting and extending techniques for proving completeness
  - Compositional proofs of KAT, KAO
  - New variant: KA with tests in a distributive lattice

Hypotheses and Closures

Hypothesis: inequation $e \leq f$ with e, f regular expressions

For a set of hypotheses H, write

$$\mathsf{KA}_H \vdash e \leq f$$

when the inequation $e \leq f$ is derivable from the axioms of Kleene algebra and the hypotheses in H (similarly for equations).

Canonical interpretation of KA with hypotheses H

Canonical interpretation of KA with hypotheses H

- We use $[\![e]\!]$ to denote the regular language belonging to regular expression e.

Canonical interpretation of KA with hypotheses H

- We use $[\![e]\!]$ to denote the regular language belonging to regular expression e.

Definition (H-closure)

(Doumane et al., Kozen and Mamouras) Let H be a set of hypotheses and $L \subseteq \Sigma^*$ a language. The *H-closure of L*, denoted as $\mathrm{cl}_H(L)$, is the smallest language containing L s.t. for all $e \leq f \in H$ and $u, v \in \Sigma^*$, if $u\,[\![f]\!]\,v \subseteq \mathrm{cl}_H(L)$, then $u\,[\![e]\!]\,v \subseteq \mathrm{cl}_H(L)$.

Canonical interpretation of KA with hypotheses H

- We use $[\![e]\!]$ to denote the regular language belonging to regular expression e.

Definition (H-closure)

(Doumane et al., Kozen and Mamouras) Let H be a set of hypotheses and $L \subseteq \Sigma^*$ a language. The *H-closure of L*, denoted as $\mathrm{cl}_H(L)$, is the smallest language containing L s.t. for all $e \leq f \in H$ and $u, v \in \Sigma^*$, if $u\,[\![f]\!]\,v \subseteq \mathrm{cl}_H(L)$, then $u\,[\![e]\!]\,v \subseteq \mathrm{cl}_H(L)$.

Example

Let $H = \{ab \leq ba, b \leq c\}$. Then, for $L = \{ca, aba\}$ we have

$$\mathrm{cl}_H(L) = \{ca, aba, ba, ab, aab\}$$

Theorem (Doumane et al. 2019, Theorem 2)

If $\mathsf{KA}_H \vdash e = f$, *then* $\mathrm{cl}_H(\llbracket e \rrbracket) = \mathrm{cl}_H(\llbracket f \rrbracket)$.

Commutative KA

$H = \{ab \leq ba \mid a, b \in \Sigma\}$. Then $\mathrm{cl}_H(L)$ is "commutative closure": $w \in \mathrm{cl}_H(L)$ iff it is a permutation of a word in L.

Examples

Commutative KA

$H = \{ab \leq ba \mid a, b \in \Sigma\}$. Then $\mathrm{cl}_H(L)$ is "commutative closure": $w \in \mathrm{cl}_H(L)$ iff it is a permutation of a word in L.

Adding a fixed language

$H = \{ab \leq 0\}$. Then $\mathrm{cl}_H(L) = L \cup \Sigma^* ab \Sigma^*$

Commutative KA

$H = \{ab \leq ba \mid a, b \in \Sigma\}$. Then $\mathrm{cl}_H(L)$ is "commutative closure": $w \in \mathrm{cl}_H(L)$ iff it is a permutation of a word in L.

Adding a fixed language

$H = \{ab \leq 0\}$. Then $\mathrm{cl}_H(L) = L \cup \Sigma^* ab \Sigma^*$

Kleene algebra with tests

$\mathsf{kat} = \mathsf{bool} \cup \mathsf{glue}$ where

$$\mathsf{glue} = \{\phi \wedge \psi = \phi \cdot \psi,\ \phi \vee \psi = \phi + \psi \mid \phi, \psi \in \mathcal{T}_{\mathrm{BA}}\} \cup \{\bot = 0,\ \top = 1\}$$

The closure is not quite the usual guarded string interpretation, but close (tbc).

The aim

Given H, investigate whether $\mathrm{cl}_H(\llbracket e \rrbracket) = \mathrm{cl}_H(\llbracket f \rrbracket)$ implies $\mathsf{KA}_H \vdash e = f$.

The aim

Given H, investigate whether $\mathrm{cl}_H(\llbracket e \rrbracket) = \mathrm{cl}_H(\llbracket f \rrbracket)$ implies $\mathsf{KA}_H \vdash e = f$.

This is not trivial: Kozen and Mamouras show that there exist cases of H for which this does not hold, and neither does decidability.

Key idea: construct a reduction from KA_H to KA.

Example

- $D = \{ab \leq 0\}$

- $D = \{ab \leq 0\}$
- $r\colon \mathcal{T}(\Sigma) \to \mathcal{T}(\Sigma)$, $r(e) = e + \Sigma^* ab \Sigma^*$.

Example

- $D = \{ab \leq 0\}$
- $r\colon \mathcal{T}(\Sigma) \to \mathcal{T}(\Sigma)$, $r(e) = e + \Sigma^* ab \Sigma^*$.
- For all e, we have $\mathsf{KA}_D \vdash e = r(e)$, and $\mathrm{cl}_D(\llbracket e \rrbracket) = \llbracket r(e) \rrbracket$.

- $D = \{ab \leq 0\}$
- $r \colon \mathcal{T}(\Sigma) \to \mathcal{T}(\Sigma)$, $r(e) = e + \Sigma^* ab \Sigma^*$.
- For all e, we have $\mathsf{KA}_D \vdash e = r(e)$, and $\mathrm{cl}_D(\llbracket e \rrbracket) = \llbracket r(e) \rrbracket$.
-

$$\begin{aligned} & \mathrm{cl}_D(\llbracket e \rrbracket) = \mathrm{cl}_D(\llbracket f \rrbracket) \\ \Leftrightarrow\ & \llbracket r(e) \rrbracket = \llbracket r(f) \rrbracket \\ \Leftrightarrow\ & \mathsf{KA} \vdash r(e) = r(f) \\ \Rightarrow\ & \mathsf{KA}_D \vdash e = f \end{aligned}$$

Definition (Reduction)

Assume $\Gamma \subseteq \Sigma$ and let H, H' be sets of hypotheses over Σ and Γ respectively. We say that H *reduces to* H' if $\mathsf{KA}_H \vdash H'$ and there exists a map $r\colon \mathcal{T}(\Sigma) \to \mathcal{T}(\Gamma)$ such that for all $e \in \mathcal{T}(\Sigma)$,

1. $\mathsf{KA}_H \vdash e = r(e)$, and
2. $\mathrm{cl}_H(\llbracket e \rrbracket) \cap \Gamma^* = \mathrm{cl}_{H'}(\llbracket r(e) \rrbracket)$.

- Simplified conditions for a reduction

- Simplified conditions for a reduction
- Summary of existing reductions: Each of the following sets of hypotheses reduce to the empty set (of hypotheses over Σ).
  (i) $\{u_i \leq w_i \mid i \in I\}$ with $u_i, w_i \in \Sigma^*$ and $|u_i| \leq 1$ for all $i \in I$
  (ii) $\{1 \leq \sum_{a \in S_i} a \mid i \in I\}$ with each $S_i \subseteq \Sigma$ finite
  (iii) $\{e \leq 0\}$ for $e \in \mathcal{T}(\Sigma)$
  (iv) $\{ea \leq a\}$ and $\{ae \leq a\}$ for $a \in \Sigma$, $e \in \mathcal{T}(\Sigma \setminus \{a\})$

- Simplified conditions for a reduction
- Summary of existing reductions: Each of the following sets of hypotheses reduce to the empty set (of hypotheses over Σ).
  (i) $\{u_i \leq w_i \mid i \in I\}$ with $u_i, w_i \in \Sigma^*$ and $|u_i| \leq 1$ for all $i \in I$
  (ii) $\{1 \leq \sum_{a \in S_i} a \mid i \in I\}$ with each $S_i \subseteq \Sigma$ finite
  (iii) $\{e \leq 0\}$ for $e \in \mathcal{T}(\Sigma)$
  (iv) $\{ea \leq a\}$ and $\{ae \leq a\}$ for $a \in \Sigma$, $e \in \mathcal{T}(\Sigma \setminus \{a\})$
- Transitivity of reductions

- Simplified conditions for a reduction
- Summary of existing reductions: Each of the following sets of hypotheses reduce to the empty set (of hypotheses over Σ).
  (i) $\{u_i \leq w_i \mid i \in I\}$ with $u_i, w_i \in \Sigma^*$ and $|u_i| \leq 1$ for all $i \in I$
  (ii) $\{1 \leq \sum_{a \in S_i} a \mid i \in I\}$ with each $S_i \subseteq \Sigma$ finite
  (iii) $\{e \leq 0\}$ for $e \in \mathcal{T}(\Sigma)$
  (iv) $\{ea \leq a\}$ and $\{ae \leq a\}$ for $a \in \Sigma$, $e \in \mathcal{T}(\Sigma \setminus \{a\})$
- Transitivity of reductions
- New tools to combine reductions

Lemma (Kappé et al. 2020)

Let $H_1, \ldots, H_n, H$ be sets of hypotheses over Σ, with $n \geq 1$. If H_i reduces to H for all i, and $\mathrm{cl}_{1 \ldots n} = \mathrm{cl}_n \circ \cdots \circ \mathrm{cl}_1$, then $\bigcup_{i \leq n} H_i$ reduces to H.

Lemma (Kappé et al. 2020)

Let $H_1, \ldots, H_n, H$ be sets of hypotheses over Σ, with $n \geq 1$. If H_i reduces to H for all i, and $\mathrm{cl}_{1 \ldots n} = \mathrm{cl}_n \circ \cdots \circ \mathrm{cl}_1$, then $\bigcup_{i \leq n} H_i$ reduces to H.

Lemma

Let $H_1, \ldots, H_n$ be sets of hypotheses, such that $\mathrm{cl}_i \circ \mathrm{cl}_j \subseteq \mathrm{cl}_j \circ \mathrm{cl}_i$ for all i, j with $i < j$. Then $\mathrm{cl}_{1 \ldots n} = \mathrm{cl}_n \circ \cdots \circ \mathrm{cl}_1$.

Lemma (Kappé et al. 2020)

Let $H_1, \ldots, H_n, H$ be sets of hypotheses over Σ, with $n \geq 1$. If H_i reduces to H for all i, and $\mathrm{cl}_{1\ldots n} = \mathrm{cl}_n \circ \cdots \circ \mathrm{cl}_1$, then $\bigcup_{i \leq n} H_i$ reduces to H.

Lemma

Let $H_1, \ldots, H_n$ be sets of hypotheses, such that $\mathrm{cl}_i \circ \mathrm{cl}_j \subseteq \mathrm{cl}_j \circ \mathrm{cl}_i$ for all i, j with $i < j$. Then $\mathrm{cl}_{1\ldots n} = \mathrm{cl}_n \circ \cdots \circ \mathrm{cl}_1$.

Lemma

For all H_1, H_2, if $\mathrm{st}_1 \circ \mathrm{cl}_2 \subseteq \mathrm{cl}_2 \circ \mathrm{cl}_1$, then $\mathrm{cl}_1 \circ \mathrm{cl}_2 \subseteq \mathrm{cl}_2 \circ \mathrm{cl}_1$.

Theorem

Let $e, f \in \mathcal{T}_{\mathsf{kat}}$. We have $\mathcal{G}(e) = \mathcal{G}(f) \Leftrightarrow \mathrm{cl}_{\mathsf{kat}}([\![e]\!]) = \mathrm{cl}_{\mathsf{kat}}([\![f]\!])$.

Theorem

Let $e, f \in \mathcal{T}_{\mathsf{kat}}$. We have $\mathcal{G}(e) = \mathcal{G}(f) \Leftrightarrow \mathrm{cl}_{\mathsf{kat}}([\![e]\!]) = \mathrm{cl}_{\mathsf{kat}}([\![f]\!])$.

$$\mathsf{atom} = \{\alpha \cdot \beta \leq 0 \mid \alpha, \beta \in \mathsf{At},\ \alpha \neq \beta\} \cup \{\alpha \leq 1 \mid \alpha \in \mathsf{At}\} \cup \{1 \leq \sum_{\alpha \in \mathsf{At}} \alpha\}$$

Theorem

Let $e, f \in \mathcal{T}_{\mathsf{kat}}$. We have $\mathcal{G}(e) = \mathcal{G}(f) \Leftrightarrow \mathrm{cl}_{\mathsf{kat}}([\![e]\!]) = \mathrm{cl}_{\mathsf{kat}}([\![f]\!])$.

$$\mathsf{atom} = \{\alpha \cdot \beta \leq 0 \mid \alpha, \beta \in \mathsf{At},\ \alpha \neq \beta\} \cup \{\alpha \leq 1 \mid \alpha \in \mathsf{At}\} \cup \{1 \leq \sum_{\alpha \in \mathsf{At}} \alpha\}$$

- kat reduces to atom

Theorem

Let $e, f \in \mathcal{T}_{\mathsf{kat}}$. We have $\mathcal{G}(e) = \mathcal{G}(f) \Leftrightarrow \mathrm{cl}_{\mathsf{kat}}([\![e]\!]) = \mathrm{cl}_{\mathsf{kat}}([\![f]\!])$.

$$\mathsf{atom} = \{\alpha \cdot \beta \leq 0 \mid \alpha, \beta \in \mathsf{At},\ \alpha \neq \beta\} \cup \{\alpha \leq 1 \mid \alpha \in \mathsf{At}\} \cup \{1 \leq \sum_{\alpha \in \mathsf{At}} \alpha\}$$

- kat reduces to atom
- For the three classes of hypotheses in atom we can show $\mathrm{cl}_{\mathsf{atom}_{1,2,3}} = \mathrm{cl}_{\mathsf{atom}_3} \circ \mathrm{cl}_{\mathsf{atom}_2} \circ \mathrm{cl}_{\mathsf{atom}_1}$

Theorem

For all $e, f \in \mathcal{T}_{\mathsf{KAT}}$, $\mathrm{cl}_{\mathsf{kat}}(\llbracket e \rrbracket) = \mathrm{cl}_{\mathsf{kat}}(\llbracket f \rrbracket)$ *implies* $\mathsf{KA}_{\mathsf{kat}} \vdash e = f$.