A cyclic proof system for Guarded Kleene Algebra with Tests

(j.w.w. Dexter Kozen & Alexandra Silva)

Jan Rooduijn

ILLC, University of Amsterdam

The Proof Society Workshop

11 November 2022
Syntax

\[ a, b ::= t \in T \mid a + b \mid a \cdot b \mid \overline{a} \mid 0 \mid 1 \]
\[ e, f ::= p \in \Sigma \mid e \cdot f \mid e +_b f \mid e^{(b)} \]
Syntax

\[ a, b ::= t \in T \mid a + b \mid a \cdot b \mid \bar{a} \mid 0 \mid 1 \]
\[ e, f ::= p \in \Sigma \mid e \cdot f \mid e +_b f \mid e^{(b)} \]

Intuition

Imperative programs
Syntax

\[ a, b ::= t \in T \mid a + b \mid a \cdot b \mid \overline{a} \mid 0 \mid 1 \]
\[ e, f ::= p \in \Sigma \mid e \cdot f \mid e +_b f \mid e^{(b)} \]

Intuition

Imperative programs

Fragments

\[ KA \subset KAT \supset GKAT \]
Semantics

At = 2^T \quad \text{GS} = \{ \alpha_0 p_1 \alpha_1 \cdots p_n \alpha_n \mid n \geq 0 \} \quad [e] \subseteq \mathcal{P}(\text{GS})
Semantics

\[ \text{At} = 2^T \]

\[ \text{GS} = \{ \alpha_0 p_1 \alpha_1 \cdots p_n \alpha_n \mid n \geq 0 \} \]

\[ \llbracket e \rrbracket \subseteq \mathcal{P}(\text{GS}) \]

**Intuition**

Atoms are states of the machine, programs are executions.
Semantics

At = 2^T 

GS = \{ \alpha_0 p_1 \alpha_1 \cdots p_n \alpha_n \mid n \geq 0 \} \quad \llbracket e \rrbracket \subseteq \mathcal{P}(GS)

Intuition

Atoms are states of the machine, programs are executions.

Determinacy

For every \( \alpha_0 p_1 x \) and \( \beta_0 q_1 y \) in \( \llbracket e \rrbracket \): \( \alpha_0 = \beta_0 \Rightarrow p_1 = q_1 \).
Example

while a do
    if b then
        p;
    else
        q;
    end
end
Example

\[
\text{while } a \text{ do } \\
\quad \text{if } b \text{ then } \\
\quad \quad p; \\
\quad \quad \text{else} \\
\quad \quad q; \\
\quad \text{end} \\
\text{end}
\]
Example

while a do
  if b then
    p;
  else
    q;
  end
end

\[ \alpha p \beta q \gamma \in [(p + b q)^{(a)}] \]
\[ \downarrow \]
\[ \alpha \leq a, b \]
\[ \beta \leq a, \bar{b} \]
\[ \gamma \leq \bar{a} \]
Some earlier results\textsuperscript{1}

\[ [e] = [f] \iff \mathcal{L}(\mathbb{A}_e) = \mathcal{L}(\mathbb{A}_f). \]

\textsuperscript{1}S. Smolka et al., \textit{Guarded Kleene algebra with tests: verification of uninterpreted programs in nearly linear time}. 
Some earlier results\(^1\)

\[ [e] = [f] \iff \mathcal{L}(\mathbb{A}_e) = \mathcal{L}(\mathbb{A}_f). \]

Equivalence of expressions is decidable is nearly linear time.

\(^1\)S. Smolka et al., *Guarded Kleene algebra with tests: verification of uninterpreted programs in nearly linear time.*
Some earlier results\textsuperscript{1}

\begin{itemize}
  \item \([e] = [f] \iff \mathcal{L}(\mathbb{A}_e) = \mathcal{L}(\mathbb{A}_f)\).
  \item Equivalence of expressions is decidable is nearly linear time.
  \item ‘Algebraic’ equational axiomatisation eGKAT:
    \[
    g \equiv eg +_b f \quad \text{e is productive} \quad \Rightarrow \quad g \equiv e^{(b)}f
    \]
\end{itemize}

\textsuperscript{1}S. Smolka et al., \textit{Guarded Kleene algebra with tests: verification of uninterpreted programs in nearly linear time}. 
Some earlier results$^1$

- $[e] = [f] \iff \mathcal{L}(\Lambda_e) = \mathcal{L}(\Lambda_f)$.
- Equivalence of expressions is decidable is nearly linear time.
- ‘Algebraic’ equational axiomatisation eGKAT:

\[
\begin{align*}
g &\equiv eg +_b f \quad \text{e is productive} \\
&\implies g \equiv e^{(b)}f
\end{align*}
\]

- Soundness: eGKAT $\vdash e \equiv f$ implies $[e] = [f]$.

---

$^1$S. Smolka et al., *Guarded Kleene algebra with tests: verification of uninterpreted programs in nearly linear time.*
Some earlier results

- $\llbracket e \rrbracket = \llbracket f \rrbracket \iff \mathcal{L}(\Lambda_e) = \mathcal{L}(\Lambda_f)$.
- Equivalence of expressions is decidable is nearly linear time.
- ‘Algebraic’ equational axiomatisation eGKAT:
  
  $g \equiv eg +_b f \quad \text{e is productive}$
  
  $g \equiv e^{(b)}f$

- Soundness: eGKAT $\vdash e \equiv f$ implies $\llbracket e \rrbracket = \llbracket f \rrbracket$.
- Completeness of eGKAT is unknown.

---

1S. Smolka et al., *Guarded Kleene algebra with tests: verification of uninterpreted programs in nearly linear time.*
<table>
<thead>
<tr>
<th>Sound</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td></td>
</tr>
</tbody>
</table>
## Proof Theory

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✅</td>
<td></td>
</tr>
</tbody>
</table>

A. Das and D. Pous, A cut-free cyclic proof system for Kleene algebra.
### Proof Theory

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✔</td>
<td>?</td>
</tr>
</tbody>
</table>

A. Das and D. Pous, A cut-free cyclic proof system for Kleene algebra.
### Proof Theory

<table>
<thead>
<tr>
<th>eGKAT</th>
<th>Sound</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>eKA</td>
<td>✓</td>
<td>?</td>
</tr>
</tbody>
</table>

A. Das and D. Pous, A cut-free cyclic proof system for Kleene algebra.
## Proof Theory

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>eKA</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

A. Das and D. Pous, A cut-free cyclic proof system for Kleene algebra.
Proof Theory

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✔</td>
<td>?</td>
</tr>
<tr>
<td>eKA</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Sound</td>
<td>Complete</td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>eGKAT</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>eKA</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Proof Theory

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
<th>Structural</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✔️</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>eKA</td>
<td>✔️</td>
<td>✔️</td>
<td>❌</td>
</tr>
</tbody>
</table>

A. Das and D. Pous, A cut-free cyclic proof system for Kleene algebra.
<table>
<thead>
<tr>
<th>Proof Theory</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
<th>Structural</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✓</td>
<td>?</td>
<td>✗</td>
</tr>
<tr>
<td>eKA</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

A. Das and D. Pous, *A cut-free cyclic proof system for Kleene algebra*. 
# Proof Theory

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
<th>Structural</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✓</td>
<td>?</td>
<td>X</td>
</tr>
<tr>
<td>eKA</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>HKA²</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
</tbody>
</table>

---

²A. Das and D. Pous, *A cut-free cyclic proof system for Kleene algebra.*
Proof Theory

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
<th>Structural</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✓</td>
<td>?</td>
<td>X</td>
</tr>
<tr>
<td>eKA</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>HKA(^2)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

\(^2\)A. Das and D. Pous, *A cut-free cyclic proof system for Kleene algebra.*
Proof Theory

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
<th>Structural</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✓</td>
<td>?</td>
<td>✗</td>
</tr>
<tr>
<td>eKA</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>HKA²</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

²A. Das and D. Pous, A cut-free cyclic proof system for Kleene algebra.
## Proof Theory

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
<th>Structural</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✓</td>
<td>?</td>
<td>✓</td>
</tr>
<tr>
<td>eKA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HKA(^2)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

\(^2\)A. Das and D. Pous, *A cut-free cyclic proof system for Kleene algebra.*
## Proof Theory

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
<th>Structural</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✓</td>
<td>?</td>
<td>✗</td>
</tr>
<tr>
<td>eKA</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>HKA$^2$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SGKAT</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

---

$^2$A. Das and D. Pous, *A cut-free cyclic proof system for Kleene algebra.*
Proof Theory

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
<th>Structural</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✓</td>
<td>?</td>
<td>✗</td>
</tr>
<tr>
<td>eKA</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>HKA(^2)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SGKAT</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

\(^2\)A. Das and D. Pous, *A cut-free cyclic proof system for Kleene algebra.*
Proof Theory

<table>
<thead>
<tr>
<th></th>
<th>Sound</th>
<th>Complete</th>
<th>Structural</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✓</td>
<td>?</td>
<td>x</td>
</tr>
<tr>
<td>eKA</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>HKA&lt;sup&gt;2&lt;/sup&gt;</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SGKAT</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

<sup>2</sup>A. Das and D. Pous, *A cut-free cyclic proof system for Kleene algebra.*
### Proof Theory

<table>
<thead>
<tr>
<th>System</th>
<th>Sound</th>
<th>Complete</th>
<th>Structural</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGKAT</td>
<td>✓</td>
<td>?</td>
<td>✗</td>
</tr>
<tr>
<td>eKA</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>HKA²</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SGKAT</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

²A. Das and D. Pous, *A cut-free cyclic proof system for Kleene algebra.*
First result: no multisets needed

SKA

\[
\frac{e \Rightarrow f}{e \Rightarrow f + g} \quad +r_1
\]

\[
\frac{e \Rightarrow g}{e \Rightarrow f + g} \quad +r_2
\]
First result: no multisets needed

SKA

\[
\frac{e \Rightarrow f}{e \Rightarrow f + g} \quad +-r_1 \quad \frac{e \Rightarrow g}{e \Rightarrow f + g} \quad +-r_2
\]

HKA

\[
\frac{e \Rightarrow [f, g]}{e \Rightarrow f + g} \quad +-r
\]
First result: no multisets needed

SKA

\[
\frac{e \Rightarrow f}{e \Rightarrow f + g} \quad +r_1
\]

\[
\frac{e \Rightarrow g}{e \Rightarrow f + g} \quad +r_2
\]

HKA

\[
\frac{e \Rightarrow [f, g]}{e \Rightarrow f + g} \quad +r
\]

SGKAT

\[
\frac{b \cdot e \Rightarrow f}{e \Rightarrow f +_{b} g} \quad +r
\]

\[
\frac{\overline{b} \cdot e \Rightarrow f}{e \Rightarrow f +_{b} g} \quad +r
\]
Future work

- What is the complexity of proof search?
Future work

- What is the complexity of proof search?
- Use SGKAT to prove completeness of eGKAT or some other algebraic axiomatisation.
Thank you!
Left logical rules

\[
\frac{\Gamma \vdash A\,\Delta}{b, \Gamma \vdash A\,\Delta} \quad b-l
\]

\[
\frac{e, \Delta}{e \cdot g, \Gamma \vdash A\,\Delta} \quad -l
\]

\[
\frac{e, \Gamma \vdash A\,\Delta}{e, \Gamma \vdash A\,\Delta} \quad e, \Gamma \vdash A\,\Delta
\]

\[
\frac{e + b f, \Gamma \vdash A\,\Delta}{e + b f, \Gamma \vdash A\,\Delta} \quad +b-l
\]

\[
\frac{e, \Gamma \vdash A\,\Delta}{e, \Gamma \vdash A\,\Delta} \quad e, \Gamma \vdash A\,\Delta
\]

\[
\frac{e, \Gamma \vdash A\,\Delta}{e, \Gamma \vdash A\,\Delta} \quad e, \Gamma \vdash A\,\Delta
\]

\[
\frac{\Gamma \vdash A\,\Delta}{\Gamma \vdash A\,\Delta} \quad \Gamma \vdash A\,\Delta
\]

Right logical rules

\[
\frac{\Gamma \vdash A\,\Delta}{\Gamma \vdash A\,\Delta} \quad b-r
\]

\[
\frac{\Gamma \vdash A\,\Delta}{\Gamma \vdash A\,\Delta} \quad \Gamma \vdash A\,\Delta
\]

\[
\frac{\Gamma \vdash A\,\Delta}{\Gamma \vdash A\,\Delta} \quad \Gamma \vdash A\,\Delta
\]

\[
\frac{\Gamma \vdash A\,\Delta}{\Gamma \vdash A\,\Delta} \quad \Gamma \vdash A\,\Delta
\]

\[
\frac{\Gamma \vdash A\,\Delta}{\Gamma \vdash A\,\Delta} \quad \Gamma \vdash A\,\Delta
\]

\[
\frac{\Gamma \vdash A\,\Delta}{\Gamma \vdash A\,\Delta} \quad \Gamma \vdash A\,\Delta
\]

Axioms and modal rule

\[
\frac{\varepsilon \Rightarrow A\,\varepsilon}{\varepsilon \Rightarrow A\,\varepsilon} \quad \text{id}
\]

\[
\frac{\Gamma \Rightarrow \emptyset\,\Delta}{\emptyset \Rightarrow A\,\Delta} \quad \bot
\]

\[
\frac{\Gamma \Rightarrow A\,\Delta}{\Gamma \Rightarrow A\,\Delta} \quad k
\]

\[
\frac{\Gamma \Rightarrow A\,\Delta}{\Gamma \Rightarrow A\,\Delta} \quad \Gamma \Rightarrow A\,\Delta
\]

\[
\frac{\Gamma \Rightarrow A\,\Delta}{\Gamma \Rightarrow A\,\Delta} \quad \Gamma \Rightarrow A\,\Delta
\]

\[
A \uparrow b = \{\alpha \in A : \alpha \leq b\}
\]

\[
(\uparrow) \ A \uparrow b = A.
\]