A cyclic proof system for Guarded Kleene Algebra with Tests

Dexter Kozen[1], **Jan Rooduijn**[2,*], **Alexandra Silva**[1]
[1]*Department of Computer Science, Cornell University, Ithaca, NY, USA*
[2]*ILLC, University of Amsterdam, The Netherlands*
[*]Email: `j.m.w.rooduijn@uva.nl`

Kleene Algebra with Tests (KAT) is a system for reasoning about program equivalence. It is a finite quasi-equational theory with two sorts, namely *programs* and a subset thereof consisting of *tests*, such that the programs form a Kleene algebra under the operations $(+, \cdot, *, 0, 1)$ and the tests form a Boolean algebra under the operations $(+, \cdot, ^{-}, 0, 1)$.

In terms of programming constructs, the operations $+, \cdot, *$ respectively capture non-deterministic choice, sequential composition and arbitrary repetition. The inclusion of tests allows one to express if-then-else statements and while loops.

Despite the gain in expressive power, the complexity of deciding KAT-equalities remains the same as for Kleene Algebra, *i.e.* it is PSPACE-complete. In [2] a fragment of KAT is identified which is computationally much more efficient, yet still reasonably expressive. This fragment, called Guarded Kleene Algebra with Tests (GKAT), is obtained by replacing the operations $+$ and * by their guarded counterparts $+_{(b)}$ and $^{(b)}$. In terms of KAT the guarded operations can be encoded as follows:

$$e +_{(b)} f \mapsto b \cdot e + \overline{b} \cdot f \qquad\qquad e^{(b)} \mapsto (b \cdot e)^* \cdot \overline{b}$$

In this talk we propose a cyclic proof system for GKAT. This system, named SGKAT, is inspired by the cyclic system in [1] for ordinary Kleene Algebra. Its rules are given on the next page. In each rule σ denotes a list of literals (*i.e.* primitive tests or their negations) and capital Greek letters denote lists of GKAT-expressions. A derivation is said to be a *proof* if every infinite branch contains infinitely many application of (b)-l.

In this talk we shall present the soundness and completeness of SGKAT with respect to the language model from [2]. Furthermore, we shall compare SGKAT to the original system in [1]. Of particular interest is that the succedents of SGKAT-sequents are lists rather than multisets of lists. Time permitting, we shall discuss the following questions of our ongoing research:

(1) What is the least possible complexity of proof search?

(2) Can SGKAT be used to prove the completeness of some algebraic axiomatisation of GKAT with respect to the language model?

$$\frac{}{\sigma, 0, \Gamma \Rightarrow \Delta}\ \text{0-}l \qquad \frac{\sigma, \Gamma \Rightarrow \Delta}{\sigma, 1, \Gamma \Rightarrow \Delta}\ \text{1-}l \qquad \frac{}{\sigma, t, \bar{t}, \Gamma \Rightarrow \Delta}\ \bot\text{-}l$$

$$\frac{\sigma, b, \Gamma \Rightarrow \Delta \qquad \sigma, c, \Gamma \Rightarrow \Delta}{\sigma, b \vee c, \Gamma \Rightarrow \Delta}\ \vee\text{-}l \qquad \frac{\sigma, e, g, \Gamma \Rightarrow \Delta}{\sigma, e \cdot g, \Gamma \Rightarrow \Delta}\ \cdot\text{-}l$$

$$\frac{\sigma, b, e, \Gamma \Rightarrow \Delta \qquad \sigma, \bar{b}, e, \Gamma \Rightarrow \Delta}{\sigma, e +_b f, \Gamma \Rightarrow \Delta}\ +_b\text{-}l$$

$$\frac{\sigma, b, e, e^{(b)}, \Gamma \Rightarrow \Delta \qquad \sigma, \bar{b}, \Gamma \Rightarrow \Delta}{\sigma, e^{(b)}, \Gamma \Rightarrow \Delta}\ (b)\text{-}l$$

$$\frac{\Gamma \Rightarrow \sigma, \Delta}{\Gamma \Rightarrow \sigma, 1, \Delta}\ \text{1-}r \qquad \frac{\Gamma \Rightarrow \sigma, e, f, \Delta}{\Gamma \Rightarrow \sigma, e \cdot f, \Delta}\ \cdot\text{-}r$$

$$\frac{b, \Gamma \Rightarrow \sigma, b, \Delta \qquad \bar{b}, \Gamma \Rightarrow \sigma, c, \Delta}{\Gamma \Rightarrow \sigma, b \vee c, \Delta}\ \vee\text{-}r_1 \qquad \frac{c, \Gamma \Rightarrow \sigma, c, \Delta \qquad \bar{c}, \Gamma \Rightarrow \sigma, b, \Delta}{\Gamma \Rightarrow \sigma, b \vee c, \Delta}\ \vee\text{-}r_2$$

$$\frac{b, \Gamma \Rightarrow \sigma, e, \Delta \qquad \bar{b}, \Gamma \Rightarrow \sigma, f, \Delta}{\Gamma \Rightarrow \sigma, e +_b f, \Delta}\ +_b\text{-}r \qquad \frac{b, \Gamma \Rightarrow \sigma, e, e^{(b)}, \Delta \qquad \bar{b}, \Gamma \Rightarrow \sigma, \Delta}{\Gamma \Rightarrow \sigma, e^{(b)}, \Delta}\ (b)\text{-}r$$

$$\frac{\Gamma \Rightarrow \Delta}{p, \Gamma \Rightarrow p, \Delta}\ \mathsf{k} \qquad \frac{}{\Rightarrow}\ \mathsf{id} \qquad \frac{b, \Gamma \Rightarrow \Delta}{b, \Gamma \Rightarrow b, \Delta}\ \mathsf{w}\text{-}r \qquad \frac{\Gamma \Rightarrow \Delta}{b, \Gamma \Rightarrow \Delta}\ \mathsf{w}\text{-}l$$

$$\frac{\Gamma \Rightarrow \sigma, b, b, \Delta}{\Gamma \Rightarrow \sigma, b, \Delta}\ \mathsf{c}\text{-}r \qquad \frac{\Gamma \Rightarrow \sigma, c, b, \Delta}{\Gamma \Rightarrow \sigma, b, c, \Delta}\ \mathsf{e}\text{-}r \qquad \frac{\sigma, b, b, \Gamma \Rightarrow \Delta}{\sigma, b, \Gamma \Rightarrow \Delta}\ \mathsf{c}\text{-}l \qquad \frac{\sigma, c, b, \Gamma \Rightarrow \Delta}{\sigma, b, c, \Gamma \Rightarrow \Delta}\ \mathsf{e}\text{-}l$$

References

[1] A. Das and D. Pous, A Cut-Free Cyclic Proof System for Kleene Algebra, in *Automated Reasoning with Analytic Tableaux and Related Methods, Brasília, Brazil, 25-28 September 2017,* pp. 261–277.

[2] S. Smolka, N. Foster, J. Hsu, T. Kappé, D. Kozen and A. Silva, Guarded Kleene algebra with tests: verification of uninterpreted programs in nearly linear time, in *ACM Symposium on Principles of Programming Languages, New Orleans, USA, 19-25 January 2020,* pp. 61:1-61:28.