One-sorted Program Algebras*

Igor Sedlár[1], and Johann J. Wannenburg[1†]

Institute of Computer Science, Czech Academy of Sciences, Prague, Czech republic
sedlar@cs.cas.cz and wannenburg@cs.cas.cz

A *Kleene algebra* [6] is an idempotent semiring $(K, \cdot, +, 1, 0)$, and hence a semilattice with partial order $x \leq y \iff x + y = y$, which is expanded with an operation $^* : K \to K$ such that

$$1 + xx^* \leq x^* \qquad y + xz \leq z \implies x^*y \leq z$$
$$1 + x^*x \leq x^* \qquad y + zx \leq z \implies yx^* \leq z.$$

A standard example of a Kleene algebra is a relational Kleene algebra where K is a set of binary relations over some set S, $\cdot$ is relational composition, $+$ is set union, * is reflexive transitive closure, 1 is identity on S and 0 is the empty set; another standard example is the Kleene algebra of regular languages over some finite alphabet.

A *Kleene algebra with tests* $\mathbf{K} = (K, B, \cdot, +, ^*, 1, 0, ^-)$, a.k.a. a *KAT*, is a two-sorted structure where $(K, \cdot, +, ^*, 1, 0)$ is a Kleene algebra, and $B \subseteq K$ with $(B, \cdot, +, ^-, 1, 0)$ a Boolean algebra [7]. The inference rules of Propositional Hoare logic (PHL) can be derived in (the equational theory of) KAT [8], i.e., it is a simple algebraic framework for verifying properties of propositional while programs. KAT is PSPACE-complete [2], has computationally attractive fragments [12], and its extensions have been applied beyond while programs, for instance in network programming languages [1].

Every Kleene algebra is a KAT; take $B = \{0, 1\}$ and define $\bar{0} = 1$ and $\bar{1} = 0$. A standard example of a KAT is a relational Kleene algebra (*rKAT*) expanded with a Boolean subalgebra of the *negative cone*, i.e. the elements $x \leq 1$, which in the relational case are subsets of the identity relation. The equational theories of KAT and rKAT coincide [9].

For various reasons, a one-sorted alternative to KAT may be desirable. For instance, "one-sorted domain semirings are easier to formalise in interactive proof assistants and apply in program verification and correctness" [4, p. 576]. A one-sorted alternative called *Kleene algebra with antidomain* was introduced in [3].

A *domain* operation [3] on a semiring $\mathbf{A}$ is any $d : K \to K$ such that

$$d(x) \leq 1 \qquad x \leq d(x)x$$
$$d(0) = 0 \qquad d(x + y) = d(x) + d(y)$$
$$d(xy) = d(xd(y)). \tag{1}$$

On a relational Kleene algebra one can define the *relational domain* operation d as follows

$$d(R) := \{(s, s) \mid \exists u.(s, u) \in R\}.$$

Then d satisfies the domain axioms above, and in fact the equational theory of domain semirings coincide with the equational theory of relation algebras in the signature $(\cdot, +, 0, 1, d)$ [10], but

*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.

†Speaker.

not the quasi-equation theory, and not necessarily in the signature which includes the Kleene-*. Informally, $d(R)$ represents the set of states in which the program associated with R has a terminating computation.

If $\mathbf{K}$ is a Kleene algebra with domain operation d, then $d(K) := \{y \mid \exists x.y = d(x)\}$ is a bounded distributive lattice contained in the negative cone in which $\cdot$ is the meet operation [3]. (It is an open problem to determine under which conditions $d(K)$ is a Heyting algebra.) In order to obtain a Boolean algebra from the distributive lattice $d(\mathbf{K})$, one has to make sure that each test $d(x)$ is complemented in $d(K)$, that is, for each $d(x)$ there is $y \in d(K)$ such that $d(x)y = 0$ and $d(x) + y = 1$. An elegant solution to this problem presented in [3] consists in expanding Kleene algebras with a single unary operation a (*antidomain*) that allows to define a domain operation d and has properties entailing that $a(x)$ is a complement of $d(x)$.

A *Kleene algebra with antidomain*, *KAA*, is a Kleene algebra expanded with an operation $a : K \to K$ such that

$$\begin{aligned} a(x)x &= 0 \\ a(xy) &\leq a(x\, a(a(y)) \\ a(x) + a(a(x)) &= 1 \end{aligned}$$

If one defines $d(x) := a(a(x))$, then d is a domain operation, and $a(x)$ is a complement of $d(x)$, so that $d(\mathbf{K}) = (d(K), \cdot, +, 1, 0)$ is a Boolean algebra [3]. On a relational Kleene algebra $a(R) = \{(w, w) \mid \neg\exists v.\, (w, v) \in R)\}$ is an antidomain operation and $a(a(R)) = d(R)$.

It is known that KAA is decidable in EXPTIME [11], and KAA can be used to create modal operators that invert the sequential composition rule of PHL. Such inversions are derivable from KAA but not KAT [13]. However, KAA has certain features that may be undesirable depending on the application. First, if $\mathbf{K}$ is a KAA, $d(\mathbf{K})$ is necessarily the maximal Boolean subalgebra of the negative cone of $\mathbf{K}$; see Thm. 8.5 in [3]. In a sense, then, every "proposition" is considered a test, contrary to some of the intuitions expressed in [7]. These intuitions also collide with the approach of taking KAT as KA with a Boolean negative cone [4, 5]. Second, not every Kleene algebra expands to a KAA, not even every finite one; see Prop. 5.3 in [3]. This is in contrast to the fact that every Kleene algebra expands to a KAT. This feature is caused by (1) (called *locality*) and the authors of [3] express interest in variants of d not satisfying (1).

In this talk we generalize KAA to a framework we'll call *one-sorted Kleene algebra with tests*. A *KAt* is a Kleene algebra expanded by two unary operations t and t' such that

$$\begin{aligned} t(0) &= 0 & t(1) &= 1 \\ t(t(x) + t(y)) &= t(x) + t(y) & t(t(x)t(y)) &= t(x)\, t(y) \\ t(x)t(x) &= t(x) & t(x) &\leq 1 \\ 1 &\leq t'(t(x)) + t(x) & t'(t(x))\, t(x) &\leq 0 \\ t'(t(x)) &= t(t'(t(x))). \end{aligned}$$

Already KAt has most of the desired features of KAA: every KAt contains a Boolean subalgebra of tests (obtained as the image of t, where t' is complementation on test elements), and the equational theory of KAT embeds into the equational theory of KAt. In addition, every Kleene algebra expands into a KAt (ensuring that it is a conservative expansion), and the subalgebra of tests in KAt is not necessarily the maximal Boolean subalgebra of the negative cone. We then consider various extensions of KAt with axioms known from KAA to show which properties of the domain operator are still consistent with the desired features of KAt. For example, the equational theory of KAT embeds into a class K of KAt's provided one of the following sufficient

conditions hold: (1) every KAT 'expands' to a member of K, or (the more restrictive) (2) every rKAT 'expands' to a member of K. We say that a KAT $\mathbf{K} = (K, B, \cdot, +, ^*, 1, 0, ^-)$ *expands* into a KAt $\mathbf{A} = (K, \cdot, +, ^*, 1, 0, t, t')$ iff $B = t(K)$. The variety of KAt's satisfy (1) while the variety of KAA's only satisfies (2). In addition, we consider a variant of the KAt framework where test complementation is defined using a residual of Kleene algebra multiplication.

References

[1] Carolyn Jane Anderson, Nate Foster, Arjun Guha, Jean-Baptiste Jeannin, Dexter Kozen, Cole Schlesinger, and David Walker. NetKAT: Semantic foundations for networks. In *Proc. 41st ACM SIGPLAN-SIGACT Symp. Principles of Programming Languages (POPL'14)*, pages 113–126, San Diego, California, USA, January 2014. ACM.

[2] Ernie Cohen, Dexter Kozen, and Frederick Smith. The complexity of Kleene algebra with tests. Technical Report TR96-1598, Computer Science Department, Cornell University, July 1996.

[3] Jules Desharnais and Georg Struth. Internal axioms for domain semirings. *Science of Computer Programming*, 76(3):181–203, 2011. Special issue on the Mathematics of Program Construction (MPC 2008). URL: https://www.sciencedirect.com/science/article/pii/S0167642310000973, doi:10.1016/j.scico.2010.05.007.

[4] Uli Fahrenberg, Christian Johansen, Georg Struth, and Krzysztof Ziemiański. Domain semirings united. *Acta Cybernetica*, pages 575–583, 2022. doi:10.14232/actacyb.291111.

[5] Peter Jipsen. From semirings to residuated Kleene lattices. *Studia Logica*, 76(2):291–303, Mar 2004. doi:10.1023/B:STUD.0000032089.54776.63.

[6] Dexter Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366 – 390, 1994. URL: http://www.sciencedirect.com/science/article/pii/S0890540184710376, doi:10.1006/inco.1994.1037.

[7] Dexter Kozen. Kleene algebra with tests. *ACM Trans. Program. Lang. Syst.*, 19(3):427–443, May 1997. doi:10.1145/256167.256195.

[8] Dexter Kozen. On Hoare logic and Kleene algebra with tests. *ACM Trans. Comput. Logic*, 1(1):60–76, July 2000. doi:10.1145/343369.343378.

[9] Dexter Kozen and Frederick Smith. Kleene algebra with tests: Completeness and decidability. In Dirk van Dalen and Marc Bezem, editors, *Computer Science Logic*, pages 244–259, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg.

[10] Brett McLean. Free kleene algebras with domain. *Journal of Logical and Algebraic Methods in Programming*, 117:100606, 2020. URL: https://www.sciencedirect.com/science/article/pii/S2352220820300912, doi:10.1016/j.jlamp.2020.100606.

[11] Bernhard Möller and Georg Struth. Algebras of modal operator and partial correctness. *Theoretical Computer Science*, 351(2):221–239, 2006. URL: https://www.sciencedirect.com/science/article/pii/S0304397505006195, doi:10.1016/j.tcs.2005.09.069.

[12] Steffen Smolka, Nate Foster, Justin Hsu, Tobias Kappé, Dexter Kozen, and Alexandra Silva. Guarded Kleene algebra with tests: Verification of uninterpreted programs in nearly linear time. In *Proc. 47th ACM SIGPLAN Symp. Principles of Programming Languages (POPL'20)*, pages 61:1–28, New Orleans, January 2020. ACM.

[13] Georg Struth. On the expressive power of Kleene algebra with domain. *Information Processing Letters*, 116(4):284–288, 2016. URL: https://www.sciencedirect.com/science/article/pii/S002001901500191X, doi:10.1016/j.ipl.2015.11.007.