Modal Kleene Algebra

Bernhard Möller

Universität Augsburg
Institut für Informatik

Collaborators: Jules Desharnais (Québec)
Thorsten Ehm, Georg Struth (Augsburg)

Partially sponsored by DFG project InopSys

1 Introduction

Aim: unify various system description calculi, such as

- relation algebra
- (multi)modal logic / PDL
- temporal logics (LTL, ITL, ...)
- sequential calculus (von Karger)
- duration calculus (Hoare/Zhou)
- predicate transformer semantics
- computation calculus (R. Dijkstra)
- ω-algebra (Cohen)
- demonic refinement algebra (von Wright)
- process algebra

Why embed this into Kleene algebra (KA)?

- particularly simple axiomatics
- more general, since it doesn't need the full concepts of a complete (Boolean) lattice, residuals or converse
- only lean versions of those
- allows a very elegant treatment

Twofold usage:

- system semantics
- system calculation

Outline:

- Basic definitions
- Modal Kleene algebras and PDL
- Modelling program correctness
- Predicate transformer algebras
- Calculating modal correspondences
- A simple greedy-like algorithm

2 Basic Definitions

Definition 2.1 [Kozen94] A *Kleene algebra (KA)* $(K, +, \cdot, ^*, 0, 1)$ is an idempotent semiring $(K, +, \cdot, 0, 1)$ with induced order

$$a \leq b \overset{\text{def}}{\Leftrightarrow} a + b = b$$

and unary operation * such that

$$1 + aa^* \leq a^* , \qquad 1 + a^*a \leq a^* ,$$
$$b + ac \leq c \Rightarrow a^*b \leq c , \qquad b + ca \leq c \Rightarrow ba^* \leq c .$$

Definition 2.2

- A *test semiring* is an idempotent semiring with a Boolean subalgebra $\text{test}(K) \subseteq K$ in which 1 is the greatest element, 0 is the least element and $\cdot$ coincides with the meet operation.
- A *(Boolean) quantale* is an idempotent semiring in which the natural order $\leq$ induces even a complete (Boolean) lattice and $\cdot$ is universally disjunctive in both arguments.
- A *Kleene algebra with tests (KAT)* [Kozen 97] is a KA in which the underlying semiring is a test semiring.

In a KAT we can give (angelic) abstract program semantics as follows:

$$\begin{aligned}
\text{abort} &\overset{\text{def}}{=} 0 \\
\text{skip} &\overset{\text{def}}{=} 1 \\
a \,[]\, b &\overset{\text{def}}{=} a + b \\
a \,;\, b &\overset{\text{def}}{=} ab \\
\text{if } p \text{ then } a \text{ else } b &\overset{\text{def}}{=} pa + \neg pb \\
\text{while } p \text{ do } a &\overset{\text{def}}{=} (pa)^*\neg p
\end{aligned}$$

For demonic semantics see below.

Definition 2.3 [Desharnais, Möller, Struth 03]
A *modal Kleene algebra (MKA)* is a KAT with an additional *domain* operation $\ulcorner\_ : K \to \text{test}(K)$ such that for all $a, b \in K$ and $p, q \in \text{test}(K)$,

$$a \leq \ulcorner a\, a , \tag{d1}$$
$$\ulcorner(pa) \leq p , \tag{d2}$$
$$\ulcorner(a\ulcorner b) \leq \ulcorner(ab) . \tag{d3}$$

Note that (d1) and (d3) can be strengthened to equalities.

(d1) and (d2) together are equivalent to each of the following:

$$\lceil a \leq p \Leftrightarrow a \leq pa, \qquad \text{(llp)}$$

$$\lceil a \leq p \Leftrightarrow \neg p a \leq 0. \qquad \text{(gla)}$$

This implies that domain commutes with all existing suprema.

A particular class of MKAs are the Boolean quantales (all sub-identities can act as tests) and hence relation algebras and path set algebras in a directed graph.

Definition 2.4 In an MKA one can define the (forward) modal operators *diamond* and *box* by

$$\langle a \rangle p \stackrel{\text{def}}{=} \lceil (ap) \ , \qquad [a]p \stackrel{\text{def}}{=} \neg \langle a \rangle \neg p \ .$$

Dually one can define a range operation $\_^\rceil$ and the backward modal operators

$$\langle\!\langle a \rangle\!\rangle p \stackrel{\text{def}}{=} (pa)^\rceil \ , \qquad [\![a]\!]p \stackrel{\text{def}}{=} \langle\!\langle a \rangle\!\rangle \neg p \ .$$

$\langle a \rangle p$ and $\langle\!\langle a \rangle\!\rangle p$ are the same as the Peirce products

- $a{:}p$ (inverse image of p under a) and
- $p{:}a$ (image of p under a),

that are the basic operations of *Kleene modules*.

Between forward and backward operators there is the important Galois connection

$$\langle\!\langle a \rangle\!\rangle p \leq q \Leftrightarrow p \leq [a]q \ . \qquad (1)$$

This implies that $\langle a \rangle$ is fully disjunctive and $[a]$ is fully conjunctive; hence both operators are monotonic and satisfy

$$\langle a \rangle 0 = 0 \ , \qquad [a]1 = 1 \ .$$

Further properties are (with $p - q \stackrel{\text{def}}{=} p\neg q$ and $p \to q \stackrel{\text{def}}{=} \neg p + q$)

$$\langle a \rangle (p - q) \geq \langle a \rangle p - \langle a \rangle q$$

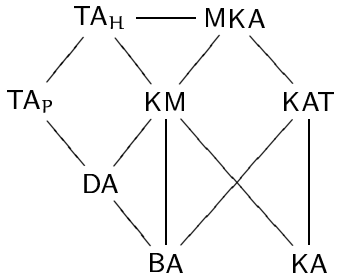
$$[a](p \to q) \leq [a]p \to [a]q$$

3 MKA and PDL

In the literature there are a number of algebraic variants of PDL:

- *dynamic algebras* DA [Pratt91]
- *Hollenberg test algebras* TA_H [Hollenberg97]
- *Pratt test algebras* TA_P [Pratt91]
- *Kleene Modules* KM [Ehm, Möller, Struth 03]

Their subsumption relations are depicted by



4 Modelling Program Correctness

It is well-known that *partial program correctness* can be modelled using the weakest liberal precondition $\mathsf{wlp}(a, q)$.

- In PDL and hence MKA this is the same as $[a]q$.
- Then a *Hoare triple* $\{p\}\ a\ \{q\}$ is *valid* if $p \leq [a]q$.
- Kozen has shown that already in KAT one can formulate validity of $\{p\}\ a\ \{q\}$ as $pa\neg q = 0$.
- Although this allows proving soundness of the rules of propositional Hoare logic (PHL), the MKA formulation leads to still simpler soundness proofs.
- Moreover, the MKA formulation admits a simple, fully algebraic proof of relative completeness of PHL [Möller, Struth 03a].

For modelling *total correctness* [Desharnais, Möller, Tchier 00], an MKA element a now receives the following interpretation:

- Its domain $\ulcorner a$ represents the set of starting states for which all a-computations are guaranteed to terminate;
- a itself represents the set of all these computation paths.
- The weakest precondition is given by

$$\mathsf{wp}(a, q) \stackrel{\mathsf{def}}{=} \ulcorner a \wedge \mathsf{wlp}(a, q)\ ,$$

- the refinement relation by

$$c \sqsubseteq a \quad \Leftrightarrow \quad \ulcorner a \leq \ulcorner c \wedge \ulcorner a \cdot c \leq a\ .$$

Demonic programming constructs:

- demonic join (choice):

$$c \sqcup a = \ulcorner a \cdot \ulcorner c \cdot (c + a)$$

- demonic meet: If $\ulcorner(c \sqcap a) = \ulcorner c \sqcap \ulcorner a$ then

$$c \sqcap a = (c \sqcap a) + \neg\ulcorner c \cdot a + \neg\ulcorner a \cdot c$$

- demonic composition:

$$c \square a \stackrel{\mathsf{def}}{=} ([c]\ulcorner a) \cdot c \cdot a$$

- demonic redefinition of loop also possible

Properties:

- Refinement: $a \sqsubseteq b \Leftrightarrow a \sqcup b = b$
- Hence we have an upper semilattice (which over a Boolean quantale is even complete).
- $\Box$ distributes through $\sqcup$ in both arguments,
- hence is $\sqsubseteq$-monotonic in both arguments.
- Associativity: $(a \Box b) \Box c = a \Box (b \Box c)$
- Over a Boolean quantale, demonic loop semantics is both $\leq$-least and $\sqsubseteq$-greatest fixpoint of its defining function [Desharnais, Möller, Tchier 00].

5 Beyond PDL: Predicate Transformer Algebras

Definition 5.1 [Möller, Struth 03b] Assume a test semiring $(K, +, \cdot, 0, 1)$.

- A *predicate transformer* is a function $f : \mathsf{test}(K) \to \mathsf{test}(K)$.
- It is *disjunctive* if $f(p + q) = f(p) + f(q)$ and *conjunctive* if $f(p \cdot q) = f(p) \cdot f(q)$. It is *strict* if $f(0) = 0$.
- Finally, id is the identity transformer and $\circ$ denotes function composition.

Let P be the set of *all* predicate transformers, M the set of monotonic and D the set of all strict and disjunctive ones.

- P forms a lattice where the join $f \oplus g$ and meet $f \sqcap g$ of f and g are the pointwise liftings of $+$ and $\cdot$:

$$(f \oplus g)(p) \stackrel{\text{def}}{=} f(p) + g(p) \;, \qquad (f \sqcap g)(p) \stackrel{\text{def}}{=} f(p)g(p) \;.$$

- The least element of P (and D) is the constant 0-valued function $\mathbf{0}$, the greatest one the constant 1-valued function $\mathbf{0}$.
- $(P, \oplus, \circ, \mathbf{0}, id)$ is an idempotent left semiring (multiplication only left-distributes over addition and is only left-strict).
- $\circ$ is even fully left-disjunctive.
- The modal operator $\langle \_ \rangle$ provides a left-semiring homomorphism from K to D.
- The substructure $(D, \oplus, \circ, \mathbf{0}, id)$ is an idempotent semiring.

Further properties (listed for the forward operators only) are:

$$\begin{array}{rclcrcl}
\langle a + b \rangle & = & \langle a \rangle \oplus \langle b \rangle \;, & & [a + b] & = & [a] \sqcap [b] \;, \\
a \leq b & \Rightarrow & \langle a \rangle \leq \langle b \rangle \;, & & a \leq b & \Rightarrow & [a] \geq [b] \;, \\
\langle pa \rangle q & = & p \langle a \rangle q \;, & & [pa] q & = & \neg p + [a] q \;, \\
\langle paq \rangle & = & \langle p \rangle \langle a \rangle \langle q \rangle \;, & & [paq] & = & [p][a][q] \;, \\
\langle ab \rangle & \leq & \langle a \rangle \langle b \rangle \;, & & [ab] & \geq & [a][b] \;.
\end{array}$$

In the presence of (d3) the last two properties can be strengthened to equalities.

If test(K) is a complete Boolean algebra then P is a complete lattice with D as a complete sublattice.

- $f^* \stackrel{\text{def}}{=} \mu g \,.\, id \oplus g \circ f \qquad {}^*f \stackrel{\text{def}}{=} \mu g \,.\, id \oplus f \circ g.$
- A KA is **-continuous* if for all a, b, c we have

$$ab^*c = \Sigma_{i \in \mathbb{N}}\, ab^i c \,.$$

- Then $f^* = \Sigma_{i \in \mathbb{N}}\, f^i$ and hence

$$f^* \leq {}^*f \,. \tag{2}$$

- The converse inequation does not hold in P, but in D.
- If h is continuous and strict then

$$h \circ f \leq f \circ h \;\Rightarrow\; h \circ f^* \leq f^* \circ h \,. \tag{3}$$

- $(P, \oplus, \circ, \mathbf{0}, id, {}^*)$ is a left KA.
- Under *-continuity, $\langle \_ \rangle$ is continuous as well.
- Since $\langle \_ \rangle$ is also strict, fixpoint fusion shows then

$$\langle a^* \rangle = \langle a \rangle^* \tag{4}$$

- So $\langle \_ \rangle$ is a homomorphism between left KAs.
- $(D, \oplus, \circ, \mathbf{0}, id, {}^*)$ is a KA, the *predicate transformer algebra*.

Definition 5.2 A KA K has *converse*, if there is an operation $\_^\smile : K \to K$ that is an involution, distributes through $+$ and is contravariant over $\cdot$, i.e., satisfies $(ab)^\smile = b^\smile a^\smile$.

Over an MKA with converse the predicate-level Galois connection (1) lifts to one between predicate transformers:

$$f \leq [a]g \;\Leftrightarrow\; \langle a^\smile \rangle f \leq g \,. \tag{5}$$

This implies the cancellation laws

$$\langle a^\smile \rangle [a] \leq \langle 1 \rangle \leq [a] \langle a^\smile \rangle \,. \tag{6}$$

6 Proving Modal Correspondences

We will first show the equivalence of the relational formulation of Noethericity with the Löb formula.

Definition 6.1 Element a is *Noetherian* if for all $p \in \text{test}(K)$,

$$p \leq \langle a \rangle p \;\Rightarrow\; p \leq 0 \,. \tag{7}$$

An equivalent formulation is

$$[a]p \leq p \;\Rightarrow\; 1 \leq p \,, \tag{8}$$

saying that the *halting predicate* $\mu p.[a]p$ is everywhere true.

The following properties have simple calculational proofs:

Lemma 6.2 *(i) 0 is Noetherian.*

(ii) If b is Noetherian and $a \leq b$, then a is Noetherian.

(iii) If a is Noetherian, then $1 \not\leq a$, that is, a is irreflexive.

(iv) 1 and a^* are not Noetherian.

(v) If $a \not\leq 0$ is Noetherian then $a \not\leq aa$, that is, a is not dense.

(vi) a is Noetherian iff a^+ is Noetherian.

Axiomatize infinite iteration [Cohen 00] by

$$a^\omega \leq aa^\omega \ ,$$
$$c \leq ac + b \Rightarrow c \leq a^\omega + a^*b \ .$$

Lemma 6.3 *Let K be an MKA that is also an ω-algebra. If a is Noetherian then $a^\omega = 0$.*

The converse implication holds only under additional assumptions.

In modal logic, Noethericity of the underlying Kripke frame is characterized by Löb's axiom

$$\Box(\Box p \to p) \to \Box p \ .$$

Defining $p \to q$ as $\neg p + q$, expressing validity of p as $p = 1$ and passing to a multimodal view, we call an element a *Löbian* if

$$[a]([a]p \to p) \to [a]p \ = \ 1 .$$

Theorem 6.4 *Let $K \in$ MKA and $a \in K$.*

(i) If a is Löbian then a is Noetherian.

(ii) If a is Noetherian and transitive then a is Löbian.

Proof (essentially due to [Goldblatt 84]): One shows that a is Noetherian iff $m = 1$, where $m \stackrel{\text{def}}{=} [a^+]([a]p \to p) \to [a]p$.

($\Leftarrow$) Assume $\langle a\rangle p \leq p$, i.e., $\langle a\rangle p \to p \ = \ 1$. Then

$$1 \ = \ [a^+]1 \to [a]p \ = \ [a]p \leq p \ .$$

($\Leftarrow$) It suffices to show that $[a]m \leq m$. First,

$$m \ = \ [a][a^*]([a]p \to p) \to [a]p \ \geq \ [a]([a^*]([a]p \to p) \to p) \ .$$

Next,

$$[a^*]([a]p \to p) \to p \ = \ ([a^+]([a]p \to p))([a]p \to p) \to p \ =$$
$$[a^+]([a]p \to p) \to (([a]p \to p) \to p) \ \geq \ m \ ,$$

since $[a]p \leq ([a]p \to p) \to p$ by shunting and modus ponens. □

Next we give an abstract proof [Möller, Struth 03b] of equivalence of the modal Geach formula and the relational confluence property.

Call an MKA *extensional* (or *separable*) if

$$a \le b \;\Leftrightarrow\; \langle a\rangle \le \langle b\rangle \;. \tag{9}$$

Theorem 6.5 *In an extensional* KAD *with converse,*

$$a^\smile b \le c\,d^\smile \Leftrightarrow\; \langle b\rangle[a] \le [a]\langle c\rangle. \tag{10}$$

Proof ($\Rightarrow$)

$$\begin{aligned} a^\smile b \le c\,d^\smile &\Leftrightarrow \langle a^\smile b\rangle \le \langle c\,d^\smile\rangle \Leftrightarrow \langle a^\smile\rangle\langle b\rangle \le \langle c\rangle\langle d^\smile\rangle \\ &\Leftrightarrow \langle b\rangle \le [a]\langle c\rangle\langle d^\smile\rangle \Rightarrow \langle b\rangle[d] \le [a]\langle c\rangle\langle d^\smile\rangle[d] \\ &\Rightarrow \langle b\rangle[d] \le [a]\langle c\rangle. \end{aligned}$$

The first step uses (9), the second step (d3), the third step (1), the fourth step monotonicity, the fifth step (6).
($\Leftarrow$) Let $\langle b\rangle[d] \le [a]\langle c\rangle$. Then

$$\langle b\rangle \le \langle b\rangle[d]\langle d^\smile\rangle \le [a]\langle c\rangle\langle d^\smile\rangle \;.$$

Then the proof continues like for ($\Rightarrow$), read upside down. □

7 A Simple Greedy-Like Algorithm

To illustrate the derivation aspect of MKA, we calculate a simple greedy-like algorithm [Möller, Struth 03b]. The motivation is relational, the derivation abstractly modal.

- Consider a specification relation T between inputs and admissible outputs.
- We seek optimal solutions, and hence use comparison relation $\sqsubseteq$ on outputs.
- The requirements on $\sqsubseteq$ will be exhibited by the derivation.

- Relation U *improves* T w.r.t. $\sqsubseteq$ if U-outputs are always at least as good as T-outputs:

$$\forall\, x,y,z : xTy \wedge xUz \Rightarrow y \sqsubseteq z \;,$$

equivalently

$$\mathrm{IMP}(U,T,\sqsubseteq) \overset{\mathrm{def}}{\Leftrightarrow} T^\smile; U \;\subseteq\; \sqsubseteq \;. \tag{11}$$

- Goal: find a sufficient criterion for

$$\mathrm{IMP}(\mathsf{while}\ P\ \mathsf{do}\ R, T, \sqsubseteq) \;.$$

How to transport the problem into the more abstract setting of (*-continuous) MKAs?

- The right hand side of (11) has the form of a confluence condition (compose $\sqsubseteq$ with $\Gamma^\smile$), which can be replaced by an instance of the Geach formula.
- Hence we set

$$\mathrm{IMP}(x,t,c) \stackrel{\mathrm{def}}{\Leftrightarrow} \langle x\rangle \leq [t]\langle c\rangle. \tag{12}$$

- Now $\mathrm{IMP}(\mathsf{while}\, p\, \mathsf{do}\, s, t, c)$ spells out to $\langle (ps)^*\neg p\rangle \leq [t]\langle c\rangle$, or equivalently, by (4),

$$\langle ps\rangle^*\langle \neg p\rangle \leq [t]\langle c\rangle\ .$$

- We abstract a bit and want to achieve, more generally $\langle v\rangle^*\langle q\rangle \leq [t]\langle c\rangle$.
- Since by (2) $\langle v\rangle^* \leq {}^*\langle v\rangle$, it suffices to show ${}^*\langle v\rangle\langle q\rangle \leq [t]\langle c\rangle$.
- By the least-fixpoint property of the left star this is implied by $\langle q\rangle \oplus \langle v\rangle[t]\langle c\rangle \leq [t]\langle c\rangle$, equivalently

$$\langle q\rangle \leq [t]\langle c\rangle \ \wedge\ \langle v\rangle[t]\langle c\rangle \leq [t]\langle c\rangle\ . \tag{13}$$

- The second conjunct, in turn, is implied by

$$\langle v\rangle[t] \leq [t]\langle c\rangle \tag{14}$$

provided $cc \leq c$.

- Note that continuity of $\langle \_\rangle$ is crucial here.

The full specification of our task in KA reads

$$\mathrm{KAOPT}(x,t,c) \stackrel{\mathrm{def}}{=} x \leq t \wedge \mathrm{IMP}(x,t,c).$$

- This yields the additional proof obligation

$$\mathsf{while}\, p\, \mathsf{do}\, s \leq t. \tag{15}$$

- Assume now that $t = \mathsf{rep}\, h \stackrel{\mathrm{def}}{=} \mathsf{while}\, \lceil h\, \mathsf{do}\, h$.
- This is for instance the case in matroids and greedoids where h is the Hasse diagram of the underlying partial order and the bases are the terminal elements w.r.t. h.
- It is easy to show that the following property implies (15):

$$ps \leq h \wedge \lceil(ps) = \lceil h. \tag{16}$$

- Next, (14) and the first conjunct of (13) spell out to

$$\langle ps\rangle[t] \leq [t]\langle c\rangle\ , \tag{17}$$

$$\langle \neg p\rangle \leq [t]\langle c\rangle\ . \tag{18}$$

- Hence, by shunting and the definition of t, condition (18) is implied by (16) if c is reflexive.

Summing up, we have

Theorem 7.1 *Suppose that* c *is a pre-order (i.e,* $1 + cc \leq c$*) and* $t = \mathsf{rep}\, h$*. If*

$$ps \leq h \wedge \lceil(ps) = \lceil h \ ,$$
$$\langle ps\rangle[t] \leq [t]\langle c\rangle \ ,$$

then

$$\mathsf{KAOPT}(\mathsf{while}\lceil h\,\mathsf{do}\, s, t, c) \ .$$

8 Conclusion

The framework of MKAs allows a unified algebraic treatment of a number of related calculi.

By ist more pristine form it avoids detours through converse and residuals, and thus in many cases leads to simpler proofs and derivations.

In the interesting and very well-behaved algebra of predicate transformers one can express properties like $\langle a^*\rangle = \langle a\rangle^*$, that cannot even be formulated in dynamic logic

Further applications of MKA and predicate transformer algebras are under way.

9 References

- J. Desharnais, B. Möller, G. Struth: Kleene algebra with domain. Tech- nical Report 2003-07, Universität Augsburg, Institut für Informatik, 2003
- J. Desharnais, B. Möller, F. Tchier: Kleene under a demonic star. In T. Rus (ed.): *Algebraic Methodology and Software Technology*, LNCS 1816, Springer 2000, pp. 355–370
- T. Ehm, B. Möller, G. Struth: Kleene modules. In R. Berghammer and B. Möller (eds.): *Participants' Proceedings 7th RelMiCS/2nd Kleene Workshop, Malente, May 12–17, 2003*, pages 21–27. Universität Kiel, Germany, 2003. Extended Version: Technical Report, Universität Augsburg, Institut für Informatik, forthcoming

- B. Möller, G. Struth: Greedy-like algorithms in Kleene algebra. In R. Berghammer and B. Möller (eds.): *Participants' Proceedings 7th RelMiCS/2nd Kleene Workshop, Malente, May 12–17, 2003*, pages 21–27. Universität Kiel, Germany, 2003. Extended Version: Technical Report, Universität Augsburg, Institut für Informatik, forthcoming
- B. Möller, G. Struth: Modal Kleene algebra and partial correctness. Technical Report 2003-08, Universität Augsburg, Institut für Informatik, 2003

- B. Möller, G. Struth: Greedy-like algorithms in Kleene algebra. In R. Berghammer and B. Möller (eds.): *Participants' Proceedings 7th RelMiCS/2nd Kleene Workshop, Malente, May 12–17, 2003*, pages 21–27. Universität Kiel, Germany, 2003. Extended Version: Technical Report, Universität Augsburg, Institut für Informatik, forthcoming