Modal Kleene Algebras

Foundations, Models, Automation

Georg Struth

University of Sheffield

based on joint work with Jules Desharnais, Peter Höfner, Bernhard Möller

Motivation

program analysis requires formalisms that balance

- expressive interoperable modelling languages
- powerful proof procedures

modelling languages: e.g.

- relations used in Z or B
- functions/quantales used in refinement calculi
- modal logics/process algebras used for reactive/concurrent systems

proof procedures dominated by

- interactive proof checking
- model checking

Motivation

questions: is there formalism that offers better balance

- unifies/integrates relational, functional, modal reasoning?
- allows using off-the-shelf automated theorem provers?

Motivation

questions: is there formalism that offers better balance

- unifies/integrates relational, functional, modal reasoning?
- allows using off-the-shelf automated theorem provers?

answer: modal Kleene algebras (maybe)

benefits of algebraic approach:

- simple equational calculus
- rich class of computationally meaningful models
- mechanisms for abstraction and (de)composition
- suitable for automation

Idempotent Semrings

i-semiring: $(S,+,\cdot,0,1)$, $+$ idempotent, $\cdot$ non-commutative

remarks: there is

- natural ordering $a \leq b \Leftrightarrow a + b = b$
- opposite semiring with multiplication swapped

test algebra: [ManesArbib] "boolean centre"

- boolean subalgebra $(\text{test}(S),+,\cdot,\neg,0,1)$ within $[0,1]$

notation: $a, b, c, \ldots$ for actions; $p, q, r, \ldots$ for tests

Kleene Algebras

Kleene algebra: [Kozen 1990] i-semiring with star satisfying

- unfold axiom $1 + aa^* \leq a^*$
- induction axiom $b + ac \leq c \Rightarrow a^*b \leq c$
- and their opposites

fact: Kleene algebra captures while-programs/guarded commands

$$\ldots$$

$$\text{if } p \text{ then } a \text{ else } b = pa + \neg pb$$

$$\text{while } p \text{ do } a = (pa)^* \neg p$$

Modal Kleene Algebras

idea:

- model state transitions via images/preimages $\langle a|p/|a\rangle p$
- complement of $|a\rangle p$ is greatest set with no a-transition into p

modal semiring: i-semiring with modal operators $S \times \mathsf{test}(S) \to \mathsf{test}(S)$ satisfying

- demodalisation axioms: $|a\rangle p \leq q \Leftrightarrow \neg q a p \leq 0 \qquad \langle a|p \leq q \Leftrightarrow p a \neg q \leq 0$
- locality axiom: $|a\rangle|b\rangle p = |ab\rangle p$

modal Kleene algebra: (MKA) modal semiring over Kleene algebra

Modalities, Symmetries, Dualities

property: modal semirings form variety (3 simple identities for $|a\rangle p \dots$)

dualities:

- de Morgan: $|a]p = \neg|a\rangle\neg p$ $\quad$ $[a|p = \neg\langle a|\neg p$
- opposition: $\langle a|$, $[a| \Leftrightarrow |a\rangle$, $|a]$

symmetries: MKAs are BAOs

- conjugation: $(|a\rangle p)q = 0 \Leftrightarrow p(\langle a|q) = 0$
- Galois: $|a\rangle p \leq q \Leftrightarrow p \leq [a|q$

benefits: rich calculus

- symmetries as theorem generators
- dualities as theorem transformers

Kleene Modules

fact: MKAs are Kleene modules

$$|a+b\rangle p = |a\rangle p + |b\rangle p \qquad |a\rangle(p+q) = |a\rangle p + |a\rangle q \qquad |ab\rangle p = |a\rangle|b\rangle p$$

$$|1\rangle p = p \qquad |a\rangle 0 = 0 \qquad |a\rangle p + q \le r \Rightarrow |a^*\rangle q \le r$$

consequence: close relationship with computational logics

Models

trace: alternating sequence $p_0 a_0 p_1 a_1 p_2 \ldots p_{n-2} a_{n-1} p_{n-1}$, $p_i \in P$, $a_i \in A$

trace product: $\sigma.p \cdot p.\sigma' = \sigma.p.\sigma'$ $\sigma.p \cdot q.\sigma'$ undefined

fact: power-set algebra $2^{(P,A)^*}$ forms (full trace) MKA

$$T_0 \cdot T_1 = \{\tau_0 \cdot \tau_1 : \tau_0 \in T_0, \tau_1 \in T_1 \text{ and } \tau_0 \cdot \tau_1 \text{ defined}\}$$

$$T^* = \{\tau_0 \cdot \tau_1 \cdot \cdots \cdot \tau_n : n \geq 0, \tau_i \in T \text{ and prods defined}\}$$

$$|T\rangle Q = \{p : p.\sigma.q \in T \text{ and } q \in Q\}$$

trace MKA**:** complete subalgebra of full trace MKA

Models

special cases: essentially by forgeting structure in trace MKA

- path/language MKAs forget actions/propositions
- relation MKAs forget sequences between endpoints

property: (equational) properties are inherited by (relations), paths, languages

further models:

- functions/predicate transformers from weaker Kleene algebras [BensonTiuryn]
- matrices over Kleene algebras [Conway/Kozen]

MKAs and PDL

fact: MKAs are dynamic/test algebras

proof: (main task) show equivalence of

- module induction law $|a\rangle p + q \leq r \Rightarrow |a^*\rangle q \leq r$
- Segerberg axiom $|a^*\rangle p - p \leq |a^*\rangle(|a\rangle p - p)$

corollary: extensional MKAs are essentially propositional dynamic logics

benefits: MKA offers

- simpler/more modular axioms
- richer model class (beyond Kripke frames)
- more flexible setting

MKAs and LTL

fact: Manna/Pnueli axioms of linear temporal logics are either

1. theorems of MKA
2. or express linearity of models (in MKA)

benefits:

- reasoning about infinite-state systems possible
- trace model available

remark: CTL also subsumed; CTL* needs additional fixedpoints

MKAs and Hore Logic

fact: MKA subsumes (propositional) Hoare logic

example: validity of while rule $\vdash_{\mathsf{MKA}} \langle a|pq \leq q \Rightarrow \langle (pa)^*\neg p|q \leq \neg pq$

benefits:

- weakest liberal precondition semantics for free in MKA ($\mathsf{wlp}(a,p) = |a]p$)
- soundness and completeness of Hoare logic easy in MKA
- idiosyncratic formalism of Hore logic superfluous

Automation

observation: modern automated theorem provers (ATPs)
have never been systematically applied to program analysis

idea: combine MKAs with ATPs and counter example generators

results: experiments with various ATPs (Prover9, SPASS, Waldmeister,. . .)

- > 300 theorems automatically proved
- successful case studies in program refinement

benefit: special-purpose calculi made redundant

Automating Hoare Logic

algorithm: integer division n/m

```
fun DIV = k:=0;l:=n;
          while m<=l do k:=k+1;l:=l-m;
```

precondition: $0 \leq n$

postconditions: $n = km + l \qquad 0 \leq l \qquad l < m$

proof goal: $\langle a_1 a_2 (r b_1 b_2)^* \neg r | p \leq q_1 q_2 \neg r$

Automating Hoare Logic

proof: two phases coupled by assignment rule $p[e/x] \leq |\{x := e\}]p$

1. MKA: goal follows from $p \leq |a_1]|a_2](q_1 q_2)$ $q_1 q_2 r \leq |b_1]|b_2](q_1 q_2)$
   (automated with Prover9)
2. arithmetics: subgoals have been manually verified, e.g.,

$$
\begin{aligned}
|a_1]|a_2](q_1q_2) &= |\{k := 0\}]\ |\{l := n\}](q_1q_2) \geq (\{n = km + l\}\{0 \leq l\})[k/0][l/n] \\
&= \{n = 0m + n\}\{0 \leq n\} = \{0 \leq n\} \\
&= p
\end{aligned}
$$

remark:

- reasoning essentially inductive
- domain specific solvers should be added to ATPs

Automating Bachmair and Dershowitz's Termination Theorem

theorem: [BachmairDershowitz86] *termination of the union of two rewrite systems can be separated into termination of the individual systems if one rewrite system quasicommutes over the other*

formalisation: Kleene module over semilattice L with infinite iteration $^\omega : K \to L$ as greatest fixedpoint

$$a^\omega \leq |a\rangle a^\omega \qquad p \leq |a\rangle p \Rightarrow p \leq a^\omega$$

encoding: $ba \leq a(a+b)^* \;\Rightarrow\; ((a+b)^\omega = 0 \Leftrightarrow a^\omega + b^\omega = 0)$

remark: posed as challenge by Ernie Cohen in 2001

Automating Bachmair and Dershowitz's Termination Theorem

results:

- SPASS takes < 5min
- proof reveals new refinement theorem

$$ba \leq a(a+b)^* \Rightarrow (a+b)^\omega = a^\omega + a^* b^\omega$$

remark: reasoning essentially coinductive

Automating a Modal Correspondence Result

modal logic: Löb's formula $\Box(\Box p \to p) \to \Box p$

translation to MKA (à la Goldblatt)

- a is pre-Löbian: $|a\rangle p \leq |aa^*\rangle(p - |a\rangle p)$
- a is Löbian: $|a\rangle p \leq |a\rangle(p - |a\rangle p)$

property: in MKA

(i) a is Löbian iff it is pre-Löbian, whenever $|a\rangle|a\rangle p \leq |a\rangle p$
(ii) $a^\omega = 0$ iff a is pre-Löbian

proof: with Prover9

(i) a few seconds
(ii) if: immediate; only if: prover runs off

Automating a Modal Correspondence Result

idea: abstract to diamond Kleene algebra

result: step-wise proof with Prover9

- following inequality can be automated ($f = |a\rangle$)

$$f - ff^*(1 - f) \leq f(f - ff^*(1 - f))$$

- claim then follows by omega coinduction and $a^\omega = 0$

remark: ATPs for inequalities should be implemented

Conclusion

this talk: modal Kleene algebras offer

- simple equational calculus incl. some (co)induction
- rich model class (traces, paths, languages, relations, functions,. . .)
- easy automation
- interesting applications in program analysis/verification

related work:

- automation of BAOs, RAs similarly successful
- code at `www.dcs.shef.ac.uk/~georg/ka`

general conclusion: ATPs

- are very suitable for algebraic reasoning
- are easy to use for research/teaching
- offer exciting perspective for non-classical logics