Omega Algebra, Demonic Refinement Algebra and Commands

Peter Höfner Bernhard Möller Kim Solin

University of Sheffield, UK

Universität Augsburg, Germany

University of Turku, Finland

Motivation

- ***demonic refinement algebra*** [vonWright04]
  - strong iteration
- ***omega algebra*** [Cohen00]
  - infinite iteration
- ***total correctness algebra*** [MöllerStruth05]
  - developed from modal Kleene algebra

what is the relationship?

Results

- interdefinability of strong and infinite iteration
- command model for demonic refinement algebra

Outline

- Relationship Between Iterations
  - demonic refinement algebra (strong iteration)
  - weak omega algebra (infinite iteration)
- Relationship Between Correctness/Refinement Algebra
  - modal Kleene algebra
  - command algebra
  - infinite iteration
- Command Model
- Conclusion

Relationship Between Iterations

Definition 1 *demonic refinement algebra* [vonWright02]

- Kleene algebra without right-zero
- strong iteration $^{\overline{\omega}}$

$$a^{\overline{\omega}} = aa^{\overline{\omega}} + 1 \qquad (\overline{\omega} \text{ unfold})$$

$$a^{\overline{\omega}} = a^* + a^{\overline{\omega}}0 \qquad (\overline{\omega} \text{ isolation})$$

$$c \leq ac + b \Rightarrow c \leq a^{\overline{\omega}}b \qquad (\overline{\omega} \text{ coinduction})$$

Remark

- greatest element $\top =_{df} 1^{\overline{\omega}}$
- $\top a = \top$

Definition 2 *weak omega algebra* [Cohen00]

- Kleene algebra without right-zero
- infinite iteration $^\omega$

$$a^\omega = aa^\omega \qquad (\omega \text{ unfold})$$

$$c \leq b + ac \Rightarrow c \leq a^\omega + a^*b \qquad (\omega \text{ coinduction})$$

Remark

- greatest element $\top =_{df} 1^\omega$
- $\top a \neq \top$

Interdefinability

Theorem 3 *strong and infinite iteration are interdefinable*

$$a^{\overline{\omega}} =_{df} a^* + a^\omega$$

$$a^\omega =_{df} a^{\overline{\omega}} 0$$

Consequences

- connect demonic refinement algebra and weak omega algebra
- knowledge transfer, e.g., command algebra

The Command Model

- idea: define *modal operators* from Kleene algebra with domain
- *modal Kleene algebra*: [MöllerStruth04]
  demodalisation/locality axiom
  $\langle a\rangle p \leq q \Leftrightarrow \neg q\, a\, p \leq 0 \qquad \langle ab\rangle p = \langle a\rangle\langle b\rangle p$
- remarks:
  - $\langle a\rangle p = \mathrm{dom}(ap)$ preimage of p under a
  - $[a]p = \neg\langle a\rangle\neg p$
  - rich calculus (based on Galois connections)
  - similar to PDL

Commands

- standard idea: command (a, p) with action $a \in S$ and termination constraint $p \in \mathsf{test}(S)$
- p models must-termination of a
- preconditions $\quad \mathsf{wlp}(a, p) =_{df} [a]p \qquad \mathsf{wp}.(a, p).q =_{df} p \cdot [a]q$

Algebra of Commands

- $$\begin{aligned} \mathsf{fail} &=_{df} (0,1) \\ \mathsf{skip} &=_{df} (1,1) \\ \mathsf{loop} &=_{df} (0,0) \\ \mathsf{chaos} &=_{df} (\top,0) \\ (a,p) \,[\!]\, (b,q) &=_{df} (a+b, pq) \\ (a,p) \,;\, (b,q) &=_{df} (ab, p \cdot [a]q) \end{aligned}$$
- $(\mathsf{COM}(S), [\!], \mathsf{fail}, ;, \mathsf{skip})$ forms weak semiring [MöllerStruth05]
- natural order: $(a,p) \leq (b,q) \Leftrightarrow a \leq b \wedge q \leq p$

Refinement Relation

- *refinement preorder*: $(a, p) \sqsubseteq (b, q) \Leftrightarrow_{df} q \leq p \wedge qa \leq b$
- $\mathsf{wp.fail.q} = 1$
  - fail is maximal w.r.t. $\sqsubseteq$
  - fail establishes any postcondition
  - fail can be interpreted as magic
- $\mathsf{wp.chaos.q} = 0$
  - chaos is refined by every command
  - chaos can be interpreted as abort

Command Kleene Algebra

Theorem 4

$$(a, p)^* =_{df} (a^*, [a^*]p)$$

yields weak Kleene algebra of commands

but what about omega?

Towards Omega

- *convergence operator* [DesharnaisMöllerStruth04]
  $\triangle : S \to \text{test}(S)$ satisfying

$$[a](\triangle a) \leq \triangle a \qquad (\triangle \text{ unfold})$$

$$q \cdot [a]p \leq p \Rightarrow \triangle a \cdot [a^*]q \leq p \qquad (\triangle \text{ induction})$$

- $\triangle a$: states without infinite a-runs

Theorem 5

$$(a, p)^\omega =_{df} (a^\omega, \triangle a \cdot [a^*]p)$$

yields weak omega algebra of commands

Demonic Refinement Algebra of Commands

putting the parts together

- interdefinability of strong and infinite iteration
- command algebra w.r.t. infinite iteration

Theorem 6 *demonic refinement algebra of commands is defined by*

$$\begin{aligned}(a,p)^{\overline{\omega}} &=_{df} (a,p)^* \mathbin{[\!]} (a,p)^\omega \\ &= (a^{\overline{\omega}}, \triangle a \cdot [a^*]p)\end{aligned}$$

Discussion

- semantic justification of demonic refinement algebra
- demonic refinement algebra does not characterise predicate transformers uniquely
- no similar move for general refinement algebra and omega algebra

Conclusion and Outlook

- links between different notions iterations
- knowledge transfer

  e.g., re-use of the existing knowledge (Kleene/omega)
- demonic refinement commmand algebra

- development of concrete refinement laws
- algebraic toolkit