Concurrent Kleene Algebras

Georg Struth

University of Sheffield

joint work with T Hoare, B Möller and I Wehrman

Motivation

Kleene algebras: models for sequential programs, refinement, action systems

process algebras: models for concurrency/communication

- axioms similar to KAs, but based on near-semirings
- $x(y+z) = xy + xz$ absent, hence no language models
- problems with axiomatisation of star
- concurrency (as interleaving) inductively defined on actions/processes

separation logic: models for local reasoning (pointer structures on heap)

- seemingly unrelated
- but separating conjunction yields conditions for sequential/concurrent executions

idea: add concurrency to Kleene algebra à la separating conjunction

Aggregation and Independency

aggregation algebra: structure $(A, +)$ with operation $+ : A \longrightarrow A$

- $p + q$ denotes system aggregated from parts p and q
- first, A absolutely free
- later it will be semigroup or monoid

independence relation: bilinear binary relation R on A

$$R(p + q, r) \Leftrightarrow R(p, r) \wedge R(q, r), \qquad R(p, q + r) \Leftrightarrow R(p, q) \wedge R(p, r)$$

- p independent of q if $R(p, q)$
- aggregate doesn't depend on system iff its parts don't dependend on it
- system doesn't depend on aggregate iff it doesn't depend on its parts

Examples

1. for aggregation algebra $(2^A, \cup)$ and $X, Y \subseteq A$, the relation $R(X, Y)$ iff X, Y disjoint is independence relation

2. for digraphs $(G, \cup)$ under (disjoint) union, $R(g_1, g_2)$ iff there is no arrow with source in g_1 and target in g_2 is independence relation

3. for subspaces of some vector space with respect to span, orthogonality is an independence relation.

4. if subtrees t_1, t_2 of tree t are in R if their roots are not on t-path and if $t_1 + t_2$ is least t-subtrees with subtrees t_1, t_2, then R is no dependence relation (subtee of $t_1 + t_2$ needn't be subtree of t_1, t_2)

Properties

lemma: for aggregation algebra $(A, +)$ and independence relation R

1. $R((p + q) + r, s) \Leftrightarrow R(p + (q + r), s)$
2. $R(p, (q + r) + s) \Leftrightarrow R(p, q + (r + s))$
3. $R(p + q, r) \Leftrightarrow R(q + p, r)$
4. $R(p, q + r) \Leftrightarrow R(p, r + q)$
5. $R(p + p, q) \Leftrightarrow R(p, q)$
6. $R(p, q + q) \Leftrightarrow R(p, q)$

Properties

proposition: relations

$$p \approx_l q \Leftrightarrow \forall r.(R(p,r) \Leftrightarrow R(q,r)) \qquad p \approx_r q \Leftrightarrow \forall r.(R(r,p) \Leftrightarrow R(r,q))$$

induce same congruence as semilattice identities on A

consequence: aggregates behave like sets with respect to independency

Properties

lemma: for aggregation algebra $(A, +)$ and independence relation R

$$R(p + q, r) \wedge R(p, q) \Leftrightarrow R(q, r) \wedge R(p, q + r)$$

proof: diagrams

consequence: write as $(p \rightarrow q) \rightarrow r = p \rightarrow (q \rightarrow r)$

Properties

lemma: for aggregation algebra $(A,+)$ and independence relations R,S with $R \subseteq S$,

1. $R(p+q,r) \wedge S(p,q) \Rightarrow S(p,q+r) \wedge R(q,r)$
2. $R(p,q+r) \wedge S(q,r) \Rightarrow S(p+q,r) \wedge R(p,q)$

proofs: use diagrams

consequence: write as

$$(p \to q) \rightsquigarrow r \leq p \to (q \rightsquigarrow r) \qquad \text{and} \qquad p \rightsquigarrow (q \to r) \leq (p \rightsquigarrow q) \to r$$

Properties

exchange law: for aggregation algebra $(A, +)$ and independence relations R, S with $R \subseteq S$ and S symmetric

$$R(p+q, r+s) \wedge S(p,q) \wedge S(r,s) \Rightarrow R(p,r) \wedge R(q,s) \wedge S(p+r, q+s)$$

proof: see diagram or calculate

$$\begin{aligned}
R(p+q, r+s) \wedge & S(p,q) \wedge S(r,s) \\
& \Leftrightarrow R(p,r) \wedge R(q,r) \wedge R(p,s) \wedge R(q,s) \wedge S(p,q) \wedge S(r,s) \\
& \Rightarrow R(p,r) \wedge S(q,r) \wedge S(p,s) \wedge R(q,s) \wedge S(p,q) \wedge S(r,s) \\
& \Rightarrow R(p,r) \wedge R(q,s) \wedge S(r,q) \wedge S(p+r,s) \wedge S(p,q) \\
& \Rightarrow R(p,r) \wedge R(q,s) \wedge S(p+r,q) \wedge S(p+r,s) \\
& \Leftrightarrow R(p,r) \wedge R(q,s) \wedge S(p+r, q+s)
\end{aligned}$$

consequence: write as $\quad (p \to q) \rightsquigarrow (r \to s) \leq (p \rightsquigarrow r) \to (q \rightsquigarrow s)$

Algebraisation

idea:

- interpret dependency arrows as algebraic operations
- lift to powerset level

extension: bistrict independence relations: $R(p, 0)$ and $R(0, p)$

complex product: for aggregation algebra $(A, +)$ and independence relation R define $\circ_R : 2^A \times 2^A \to 2^A$ by

$$X \circ_R Y = \{p + q : p \in X \wedge q \in Y \wedge R(p, q)\}$$

example: if X, Y are languages, $+$ is string concatenation and R is universal relation, then $\circ_R$ is language product

Algebraisation

proposition:

1. if $(A, +)$ is semigroup and R bilinear, then $(2^A, \circ_R)$ is semigroup
2. if $(A, +, 0)$ is monoid and R bilinear bistrict, then $(2^A, \circ_R, \{0\})$ is monoid

proof: simple but tedious (using relation-level "associativity")...

proposition:

1. if $(A, +)$ is semigroup and R bilinear, then $(2^A, \cup, \circ_R, \emptyset)$ is dioid
2. if $(A, +, 0)$ is monoid and R bilinear bistrict, then $(2^A, \cup, \circ_R, \emptyset, \{0\})$ is dioid with 1

proof: set theory...

remark: even infinite distributivity laws hold

Algebraisation

theorem: if $(A, +, 0)$ is monoid and R bilinear bistrict, then $(2^A, \cup, \circ_R, \emptyset, \{0\}, {}^*)$ is Kleene algebra, where

$$X^* = \bigcup_{i \geq 0} X^i$$

as in language theory

proof:

- X^* exists by completeness of semilattice reduct of dioid
- verifying KA star axioms is routine

discussion: KA deals with sequentiality in the sense that parts of a system can be aggregated "before" other parts only if the former don't depend on the latter

Modelling Concurrency

idea: make independency relation symmetric

- complex product $X \circ_S Y = \{p + q : p \in X \wedge q \in Y \wedge S(p, q)\}$ only aggregates elements that are mutually independent
- in that case, p and q can be executed concurrently

lemma: if $(A, +)$ is semigroup and S bilinear symmetric, then $(2^A, \circ_S)$ is commutative semigroup

theorem: if $(A, +, 0)$ is monoid and S bilinear bistrict symmetric, then $(2^A, \cup, \circ_S, \emptyset, \{0\}, ^\star)$ is commutative Kleene algebra

remark: commutative KAs have been studied by Conway/Pilling

Concurrent Kleene Algebras

idea: combine sequential and concurrent composition

definition:

- bisemigroup : $(S, \bullet, \circ)$ with $(S, \bullet)$ and $(S, \circ)$ semigroups
- bimonoid: $(S, \bullet, \circ, 1)$ with $(S, \bullet, 1)$ and $(S, \circ, 1)$ monoids
- trioid: $(S, +, \bullet, \circ, 0, 1)$ with $(S, +, \bullet, 0, 1)$ and $(S, +, \circ, 0)$ dioids
- bi-Kleene algebra: $(S, +, \bullet, \circ, {}^*, {}^\star, 0, 1)$ with $(S, +, \bullet, {}^*, 0, 1)$ and $(S, +, \circ, {}^\star, 0, 1)$ KAs

theorem: if $(A, +, 0)$ is monoid, R, S bilinear bistrict, then

- $(2^A, \cup, \circ_R, \circ_S, \emptyset, \{0\})$ is trioid
- $(2^A, \cup, \circ_R, \circ_S, {}^*, {}^\star, \emptyset, \{0\})$ is bi-KA

Concurrent Kleene Algebras

but: structure of R, S not taken into account

- S symmetric, hence $\circ_S$ commutative
- $R \subseteq S$, hence $X \circ_R Y \subseteq X \circ_S Y$

lemma: if $(A, +)$ semigroup and R, S bilinear with $R \subseteq S$, then

1. $(x \circ_S y) \circ_R z \subseteq x \circ_S (y \circ_R z)$
2. $x \circ_R (y \circ_S z) \subseteq (x \circ_R y) \circ_S z$

proof: use $R(p + q, r) \wedge S(p, q) \Rightarrow S(p, q + r) \wedge R(q, r)$ and its dual

Concurrent Kleene Algebras

exchange law: if $(A, +)$ semigroup, R, S bilinear, $R \subseteq S$ and S symmetric, then

$$(w \circ_S x) \circ_R (y \circ_S z) \subseteq (w \circ_R y) \circ_S (x \circ_R z)$$

proof: use $R(p+q, r+s) \wedge S(p,q) \wedge S(r,s) \Rightarrow R(p,r) \wedge R(q,s) \wedge S(p+r, q+s)$

remark: lifting of relational properties to algebraic properties

Concurrent Kleene Algebras

definition:

- concurrent semigroup: ordered bisemigroup $(S, \bullet, \circ)$ that satisfies

$$x \bullet y \le x \circ y, \qquad x \circ y = y \circ x,$$
$$(x \circ y) \bullet z \le x \circ (y \bullet z), \qquad x \bullet (y \circ z) \le (x \bullet y) \circ z,$$
$$(w \circ x) \bullet (y \circ z) \le (w \bullet y) \circ (x \bullet z)$$

- concurrent monoid: ordered bimonoid $(S, \bullet, \circ, 1)$ that satisfies

$$x \bullet y \le x \circ y, \qquad x \circ y = y \circ x, \qquad (w \circ x) \bullet (y \circ z) \le (w \bullet y) \circ (x \bullet z)$$

lemma: $(x \circ y) \bullet z \le x \circ (y \bullet z)$ and $x \bullet (y \circ z) \le (x \bullet y) \circ z$ hold in concurrent monoids

Concurrent Kleene Algebras

concurrent Kleene algebra: bi-KA $(S, +, \bullet, \circ, ^*, ^\star, 0, 1)$ over concurrent monoid

therefore: CKAs consist of KA and commutative KA that interact as follows:

- sequential composition includes concurrent composition
- exchange law holds

theorem: if $(A, +, 0)$ monoid, R, S bilinear bistrict, $R \subseteq S$ and S symmetric, then $(2^A, \cup, \circ_R, \circ_S, ^*, ^\star, \emptyset, \{0\})$ is concurrent Kleene algebra

proof:

- again only monoid case is interesting (see above lemmas)
- stars exist/defined due to infinite distributivity laws

Sequential and Concurrent Compositions

aggregation algebra: distributive lattice $(A, +, \cdot, 0)$ with operator $f : A \to A$

example: f (pre)image operator on relational structure

composition operations:

- fine-grain concurrent composition $X \star Y$ with $R_\star(p, q) \Leftrightarrow p \cdot q = 0$
  (dependencies between X and Y ignored)
- weak sequential composition $X ; Y$ with $R_;(p, q) \Leftrightarrow R_\star(p, q) \wedge f(p) \cdot q = 0$
  (no dependency of X on Y)
- disjoint parallel composition $X || Y$ with $R_{||}(p, q) \Leftrightarrow R_;(p, q) \wedge p \cdot f(q) = 0$
  (no dependency in either direction)
- alternation $X \oplus Y$ with $R_\oplus(p, q) \Leftrightarrow p = 0 \vee q = 0$
  (at most one of X, Y executed)

Sequential and Concurrent Compositions

lemma:

1. $R_{\oplus} \subseteq R_{||} \subseteq R_{;} \subseteq R_{\star}$
2. all compositions are bilinear bistrict
3. all except $R_{;}$ are symmetric

consequence: for $(A, +, \cdot, 0, f)$ and any concurrent composition relation R_C,
$(2^A, \cup, ;, \circ_C, {}^*, {}^C, \emptyset, \{0\})$ is CKA

remark: sometimes dual order needs to be taken

question: is independency model canonical?

Shuffle Dioids

shuffle dioid: dioid $(S, +, \cdot, 0, 1)$ finitely generated by finite Σ and with shuffle operation $\otimes : S \to S$ satisfying

$$1 \otimes x = x = x \otimes 1, \qquad ax \otimes by = a(x \otimes by) + b(ax \otimes y),$$
$$x \otimes (y + z) = x \otimes y + x \otimes z$$

analogy: process algebras such as ACP, CCS

related model: regular languages under regular operations plus shuffle

$$\epsilon \otimes w = \{w\} = w \otimes \epsilon, \qquad av \otimes bw = \{a(v \otimes bw), b(av \otimes w)\},$$
$$X \otimes Y = \bigcup \{v \otimes w : v \in X \wedge w \in Y\}$$

Shuffle Dioids

lemma: $(S, +, \otimes, 0, 1)$ is commutative dioid.

proof: by induction, e.g.,

$$ax \otimes by = a(x \otimes by) + b(ax \otimes y) = b(y \otimes ax) + a(by \otimes x) = by \otimes ax$$

lemma: $xy \leq x \otimes y$

proof: e.g. $axby \leq a(x \otimes by) \leq a(x \otimes by) + b(ax \otimes y) = ax \otimes by$

Shuffle Dioids

lemma: exchange law $(w \otimes x)(y \otimes z) \leq wy \otimes xz$

proof: e.g.

$$\begin{aligned}(aw \otimes bx)(y \otimes z) &= a(w \otimes bx)(y \otimes z) + b(aw \otimes x)(y \otimes z) \\ &\leq a(wy \otimes bxz) + b(awy \otimes xz) \\ &= awy \otimes bxz\end{aligned}$$

theorem: shuffle dioids (regular languages with shuffle) are concurrent semirings

Free Concurrent Semirings

question: are regular languages with shuffle the free CKAs?

fact: in language model, exchange law is essentially inequation:

$$(a \otimes a)(b \otimes b) = \{aabb\} < \{aabb, abab\} = ab \otimes ab$$

lemma: in every CKA, $v(x \otimes wy) + w(vx \otimes y) \leq vx \otimes wy$

proof: by ATP

intuition: algebraic version of shuffle induction

Free Concurrent Semirings

but: converse inequality fails in CKA

proof: In CKA $S = \{a\}$ with $0 \leq a \leq 1$, $aa = a$ and $a \otimes a = 1$,

$$a1 \otimes a1 = a \otimes a = 1 > a = aa + aa = a(1 \otimes a1) + a(a1 \otimes 1)$$

consequence: CKA is strict superclass of shuffle dioids

question: how can we eliminate $\otimes$ in CKA?

Free Concurrent Semirings

lemma: following equation doesn't hold in CKA, but it holds in shuffle semirings:

$$xy \otimes xy \leq x \otimes x(y \otimes y)$$

proof: consider CKA over $\{a, b\}$ defined by $0 < a < b < 1$ and tables

$\cdot$	0	a	b	1
0	0	0	0	0
a	0	a	a	a
b	0	a	a	b
1	0	a	b	1

$\otimes$	0	a	b	1
0	0	0	0	0
a	0	1	b	a
b	0	b	b	b
1	0	a	b	1

then $bb \otimes bb = a \otimes a = 1 > b = b \otimes a = b \otimes bb = b \otimes b(b \otimes b)$

Free Concurrent Semirings

proof continued: but in regular languages with shuffle, in

$$xy \otimes xy \leq x \otimes x(y \otimes y)$$

- at least one x must first be eaten before consuming y in lhs
- this can be simulated by rhs

consequence: regular languages with shuffle are not free CKAs!

questions:

- what are free CKAs?
- can CKA be extended to characterize shuffle languages?

Conclusion

CKA: extension of KA to concurrent setting

- two models (independency/aggregation, shuffle languages)
- formalisms like Hoare logic and rely/guarantee calculus can be modelled

interesting questions:

- free algebras
- decidability
- expressivity