Kleene Algebra

Georg Struth
University of Sheffield, UK

Outline

plan

- give overview of field
- focus on mathematical techniques rather than axiomatisations
- discuss computing applications in exercise sessions?
- use Isabelle for proving theorems in exercises?
- slides only as guidance; proofs/examples on blackboard

topics

1. Kleene algebras and regular algebras
2. modal Kleene algebras
3. concurrent Kleene algebras
4. towards concurrent separation logic

Kleene Algebras and Regular Algebras

- Part I -

Motivation

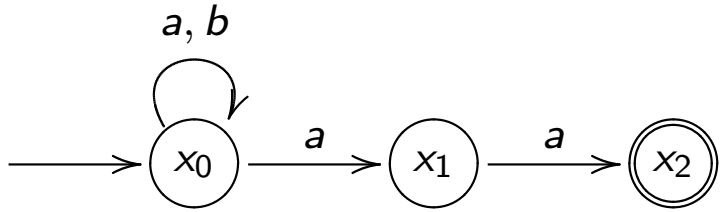
regular algebra

- regular expressions $t ::= 0 \mid 1 \mid a \in \Sigma \mid t + t \mid t \cdot t \mid t^*$
- interpretation $L : \mathsf{RegExp} \to \mathsf{RegLan}$
- question: axiomatise $s \approx t \Leftrightarrow L(s) = L(t)$ (trace equivalence)

Motivation

regular equations

- automaton



- recursive language equations

$$x_0 = (a + b)x_0 + ax_1 \qquad x_1 = ax_2 \qquad x_2 = 1$$

- Arden's rule $y = xy + z \Rightarrow y = x^*z$ if $\neg \text{ewp } x$ yields solution

$$x_0 = (a + b)^* aa1 = (a + b)^* aa$$

- question: what is underlying algebra?

Regular Algebras

axioms

- based on dioids (idempotent semirings) $(S, +, \cdot, 0, 1)$
  - $(S, +, 0)$ is semilattice with least element 0
  - $(S, \cdot, 1)$ is monoid
  - $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$
  - $x0 = 0$ and $0x = 0$

$$x + (y + z) = (x + y) + z \qquad x + y = y + x \qquad x + 0 = x \qquad x + x = x$$

$$x(yz) = (xy)z \qquad x1 = x \qquad 1x = x$$

$$x(y + z) = xy + xz \qquad (x + y)z = xz + yz$$

$$x0 = 0 \qquad 0x = 0$$

Regular Algebras

natural order

- define

$$x \leq y \Leftrightarrow x + y = y$$

- this yields partial order since $(S, +)$ is semilattice
- regular operations preserve order (e.g. $x \leq y \Rightarrow z + x \leq z + y$)
- 0 is least element

further properties

- natural order is only order with these properties
- $x \sqsubseteq y \Leftrightarrow \exists z.x + z = y$ defines same relation

Regular Algebras

opposition

- consider endo $\partial : S \to S$ defined by

  $$\partial(0) = 0 \quad \partial(1) = 1 \quad \partial(x + y) = \partial(x) + \partial(y) \quad \partial(x \cdot y) = \partial(y) \cdot \partial(x)$$

  which swaps order of multiplication
- $\partial(S)$ is again a dioid; the opposite dioid

remark

this could be implemented by operation of conversion

$$0^\circ = 0 \qquad 1^\circ = 1 \qquad (x + y)^\circ = x^\circ + y^\circ$$
$$(xy)^\circ = y^\circ x^\circ \qquad x^{\circ\circ} = x \quad \ldots$$

Regular Algebras

free dioids

- are $\cong$ sets of words (languages)
- nice term normal forms due to distributivity laws
  - $(x + y)z = xz + yz$ yields trees
  - $x(y + z) = xy + xz$ pushes $+$-nodes towards root

task

- axiomatise *
- Redko: variety not finitely axiomatisable
- answer: Salomaa, Conway, Krob, Kozen, Boffa, ...
- next slides ...

Regular Expression and Regular Languages Recap

terms

regular expressions over Σ form ground terms $T_R(\Sigma)$ of regular algebra

notation

Σ^* denotes free monoid with empty word ϵ over Σ
(set of all words/strings)

interpretation

map $L : T_R(\Sigma) \to 2^{\Sigma^*}$ induces regular languages over Σ:

$$L(0) = \emptyset \qquad L(1) = \{\epsilon\} \qquad L(a) = \{a\} \text{ for } a \in \Sigma$$
$$L(s + t) = L(s) \cup L(t) \qquad L(s \cdot t) = L(s) \cdot L(t) \qquad L(t^*) = L(t)^*$$

where, for $X, Y \subseteq \Sigma^*$,

$$X \cdot Y = \{vw : v \in X \wedge w \in Y\} \quad X^0 = \{\epsilon\} \quad X^{i+1} = XX^i \quad X^* = \bigcup_{i \geq 0} X^i$$

Empty Word Property

languages

language X has empty word property if $\epsilon \in X$

regular expressions

$$ewp(1) \quad \neg\text{ewp}(0) \qquad \neg\text{ewp}(a) \qquad \text{ewp}(s^*)$$

$$\text{ewp}(s+t) \Leftrightarrow \text{ewp}(s) \vee \text{ewp}(t) \qquad \text{ewp}(st) \Leftrightarrow \text{ewp}(s) \wedge \text{ewp}(t)$$

then $ewp(t) \Leftrightarrow \epsilon \in L(t)$

Salomaa's Axioms

axioms

let $r, s, t \in T_R(\Sigma)$

- equational axiom schemes

$$r + (s + t) = (r + s) + t \qquad r(st) = (rs)t \qquad r + s = s + r$$
$$r(s + t) = rs + rt \qquad (r + s)t = rt + st \qquad r + r = r$$
$$0^* r = r \qquad 0r = 0 \qquad 0 + r = r \qquad r^* = 0^* + r^* r \qquad r^* = (0^* + r)^*$$

- substitution of equations: let $t' = t[s/r]$

$$r = s \wedge t = u \;\Rightarrow\; t' = u \wedge t' = t$$

- Arden's rule

$$\neg \mathrm{ewp}(s) \Rightarrow r = rs + t \Rightarrow r = ts^*$$

remark

star-free axioms are equivalent to instances of dioid axioms

Salomaa's Axioms

soundness

- the structure $(2^{\Sigma^*}, \cup, \cdot, ^*, \emptyset, \{\epsilon\})$ forms a model of Salomaa's axioms
- we call this the full language regular algebra over Σ
- every subalgebra of this is also a model
- we call these language regular algebras
- in particular the set of all regular languages over Σ forms a model

consequence

if $s = t$ follows from Salomaa's axioms, then $L(s) = L(t)$

Salomaa's Axioms

completeness

if $L(s) = L(t)$, then $s = t$ follows from Salomaa's axioms

proof sketch

1. two finite sets of characteristic linear equations are derivable

$$s = \sum_{i=1}^{r} s_i x_i + \delta(s) \qquad t = \sum_{i=1}^{r} t_i x_i + \delta(t)$$

$$s_1 = \sum_{j=1}^{r} s_{1j} x_j + \delta(s_1) \qquad t_1 = \sum_{j=1}^{r} t_{1j} x_j + \delta(t_1)$$

$$\ldots \qquad \ldots$$

2. all $L(s_i) = L(t_i)$ are recursively valid (by soundness)
3. derivable solutions of regular equations are unique (Arden's rule)
4. hence $s = t$ is derivable

details on blackboard

Conway's Axioms

classical axioms

- dioid axioms (essentially)
- star axioms

$$(x+y)^* = (x^*y)^*x^* \qquad (xy)^* = 1 + x(yx)^*y \qquad x^* = (x^{n+1})^* \sum_{i=0}^{n} x^i$$

- but these are incomplete

conjectures

- various extensions, e.g. by $z + xy \leq y \Rightarrow x^*z \leq y$ and dual
- Krob proved completeness of extension by "monoid identities"

Kozen's Axioms

Kleene algebras

dioids with star axioms

$$1 + xx^* \leq x^* \qquad z + xy \leq y \Rightarrow x^*z \leq y$$

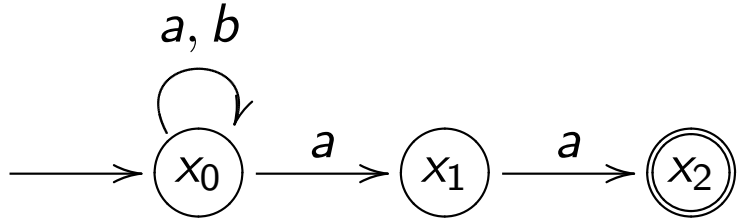
and opposites

soundess

regular languages form model
(Kozen's axioms derivable from Salomaa's)

Completeness of Kozen's Axioms

automata as matrices



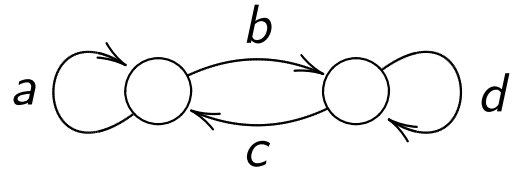
$$\left[\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} a+b & a & 0 \\ 0 & 0 & a \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right]$$

Completeness of Kozen's Axioms

theorem

- let $M_n(K)$ denote $n \times n$ matrices over Kleene algebra K
- let Z_n and I_n be $n \times n$ zero and identity matrix
- then $(M_n(K), +, \cdot, ^*, Z_n, I_n)$ is Kleene algebra

star



$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad M^* = \begin{pmatrix} f^* & f^*bd^* \\ d^*cf^* & d^* + d^*cf^*bd^* \end{pmatrix}$$

for $f = a + bd^*c$
partition larger matrices into submatrices with squares along diagonal

Example

in our previous example we split

$$\left(\begin{array}{c|cc} a+b & a & 0 \\ \hline 0 & 0 & a \\ 0 & 0 & 0 \end{array}\right)$$

and first compute

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}^*$$

now $f = 0 + 0 = 0$ and therefore the solution is

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

we now compute f for the 3×3-matrix

$$f = (a+b) + \begin{pmatrix} a & 0 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} = a + b$$

Example

for the other parts of the star matrix we obtain

$$(a+b)^* \begin{pmatrix} a & 0 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = (a+b)^* \begin{pmatrix} a & aa \end{pmatrix} = \begin{pmatrix} (a+b)^* a & (a+b)^* aa \end{pmatrix}$$

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \end{pmatrix} (a+b)^* = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} (a+b)^* \begin{pmatrix} a & 0 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \cdots = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

this yields

$$\begin{pmatrix} a+b & a & 0 \\ 0 & 0 & a \\ 0 & 0 & 0 \end{pmatrix}^* = \begin{pmatrix} (a+b)^* & (a+b)^* a & (a+b)^* aa \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}$$

Completeness of Kozen's Axioms

acceptance

automaton $[i, M, f]$ accepts language $L(i^T M^* f)$

example

$$\begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a+b & a & 0 \\ 0 & 0 & a \\ 0 & 0 & 0 \end{pmatrix}^* \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} (a+b)^* & (a+b)^* a & (a+b)^* aa \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} (a+b)^* aa \\ a \\ 1 \end{pmatrix}$$

$$= (a+b)^* aa$$

Completeness of Kozen's Axioms

lemma

every M can be written, for boolean matrices J and M_a, as

$$M = J + \sum_{a \in \Sigma} a M_a$$

remark

this yields characteristic matrix equation

lemma

every t satisfies $t = i^T M^* f$ for some automaton of this form
(replay one half of Kleene's theorem at matrix level)

Completeness of Kozen's Axioms

theorem

the following constructions are theorems of Kleene algebra

1. for every $[i_1, M_1, f_1]$ exists ϵ-free $[i_2, M_2, f_2]$ with $i_1^T M_1^* f_1 = i_2^T M_2^* f_2$ (by simple matrix algebra)
2. for every such $[i_2, M_2, f_2]$ exists deterministic $[i_3, M_3, f_3]$ with $i_2^T M_2^* f_2 = i_3^T M_3^* f_3$ (by simulating subset construction)
3. for every such $[i_3, M_3, f_3]$ exists minimal $[i_4, M_4, f_4]$ with $i_3^T M_3^* f_3 = i_4^T M_4^* f_4$ (by dividing by Myhill-Nerode relation)

remark

(2) and (3) use coercion matrices to map $XM_i = M_{i+1}X$

Completeness of Kozen's Axioms

completeness theorem

$L(s) = L(t)$ implies $s = t$ is theorem of Kleene algebra

proof

- let s and t denote the same set
- let $[i_s, M_s, f_s]$ and $[i_t, M_t, f_t]$ be minimal DFAs that satisfy

$$s = i_s^T M_s^* f_s \qquad t = i_t^T M_t^* f_t$$

- then they are isomorphic, so there is permutation matrix P with

$$M_s = P^T M_t P \qquad i_s = P^T i_t \qquad f_s = P^T f_t$$

- thus, in KA,

$$s = i_s^T M_s^* f_s = (P^T i_t)^T (P^T M_t P)^* (P^T f_t) = \cdots = t$$

Boffa's Axioms

first axiom system

dioid plus star axioms

$$(x+y)^* = (x^*y)^*x^* \qquad (xy)^* = 1 + x(yx)^*y \qquad xx = x \Rightarrow x^* = 1 + x$$

second axiom system

dioid plus "reflexive transitive closure" star axioms

$$1 + x \leq x^* \qquad x^*x^* = x^* \qquad 1 + x \leq y \wedge yy = y \Rightarrow x^* \leq y$$

theorem

- axiom systems are interderivable
- both are complete (relative to Krob's result)

Left Kleene Algebras

left Kleene algebras

dioids with star axioms

$$1 + xx^* \leq x^* \qquad z + xy \leq y \Rightarrow x^*z \leq y$$

without opposites

theorem

left Kleene algebras are complete

proof

- Boffa's axioms are derivable (completeness relative to Krob's result)
- Kozen and Silva via matrices and coalgebra

fine structure of regular algebra

[Foster/Struth, ICJAR 2012]

Models of Kleene Algebra

boolean semiring

structure $A_2 = (\{0,1\}, +, \cdot, ^*, 0, 1)$ with operations

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

$$0^* = 1^* = 1$$

bounded distributive lattice

$(D, \sqcup, \sqcap, 0, 1, ^*)$ with $x^* = 1$ for all $x \in D$

Models of Kleene Algebra

binary relation

set of ordered pairs on set A

$$R = \{(a, b) : a, b \in A\}$$

operations

$$\Delta = \{(a, a) : a \in A\}$$

$$R \circ S = \{(a, b) : \exists c.(a, c) \in R \wedge (c, b) \in S\} \qquad R^* = \bigcup_{i \geq 0} R^i$$

remark

R^* is reflexive transitive closure of R

Models of Kleene Algebra

theorem

- $(2^{A \times A}, \cup, \circ, {}^*, \emptyset, \Delta)$ is a Kleene algebra, the full relation Kleene algebra over A
- every subalgebra of a full relation Kleene algebra is a relation Kleene algebra

remark

- obviously ewp doesn't make sense here...
- binary relations yield standard semantics for (imperative) programs

Models of Kleene Algebra

paths in digraphs

- finite sequences of states from digraph $G = (V, E)$ that follow edges
- empty path ϵ

path products

glue paths on initial/final state

$$\sigma.p \cdot p.\sigma' = \sigma.p.\sigma' \qquad \sigma.p \cdot q.\sigma' \quad \text{undefined}$$

lifting to sets

- $P_1 \circ P_2 = \{\pi_1 \cdot \pi_2 : \pi_1 \in P_1, \pi_2 \in P_2 \text{ and } \pi_1 \cdot \pi_2 \text{ defined}\}$
- other operations as usual

theorem

(suitable) sets of paths form path Kleene algebras

Models of Kleene Algebra

traces

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

lifting to sets

- $T_1 \circ T_2 = \{\tau_1 \cdot \tau_2 : \tau_1 \in T_1, \tau_2 \in T_2 \text{ and } \tau_1 \cdot \tau_2 \text{ defined}\}$
- other operations as usual

theorem

(suitable) sets of traces form trace Kleene algebras

Relationship Between Models

relationship

essentially by forgetting structure in trace algebras

- path/language Kleene algebras forget actions/propositions
- relation Kleene algebras forget everything between endpoints

theorem

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

read more

[HöfnerStruth JLAP 2010]

Kleene Algebras

other models

- matrices (as we have seen)
- formal power series
- tropical (min-plus) semiring $(N_\infty, \min, +, \infty, 0, ^*)$ forms Kleene algebra if $n^* = 0$ for all $n \in N_\infty$

tropical semirings

- applications in graph algorithms, combinatorial optimisation, internet routing
- this would require another lecture series...
- max-plus semiring cannot be expanded to Kleene algebra

Other Results

theorem

equational theory of relational and language KA is the same

- use Cayley map $c(L) = \{(x, xy) : x \in \Sigma^*, y \in L\}$

quasivariety of KA

undecidable (uniform word problem for semigroups)

quasivariety of regular expressions

KA doesn't work

- $x^2 = 1 \Rightarrow x = 1$ holds in language KA
- but not for relation $R = \{(0, 1), (1, 0)\}$, which form KA (with $\{(0, 0), (1, 1)\}$, $\emptyset$, etc.)

Modelling Example

Church-Rosser theorem

$y^*x^* \leq x^*y^* \Rightarrow (x+y)^* \leq x^*y^*$

proof

induction on number of peaks

$$
\begin{aligned}
(x+y)^* \leq x^*y^* &\Leftrightarrow (y^*x^*)^* \leq x^*y^* && \text{(regular identity)} \\
&\Leftarrow 1 + y^*x^*x^*y^* \leq x^*y^* && \text{(induction)} \\
&\Leftrightarrow 1 \leq x^*y^* \ \wedge \ y^*x^*x^*y^* \leq x^*y^* && \text{(lub)}
\end{aligned}
$$

- base case: $1 \leq x^*y^*$ trivial
- induction step: $y^*x^*x^*y^* = y^*x^*y^* \leq x^*y^*y^* = x^*y^*$

Kleene Algebras with Tests

program analysis

- reason about actions and propositions/states
- use KA for actions and BA for state space

idea

two-sorted structre $(K, B, +, \cdot, 0, 1, ^*)$

- BA $(B, +, \cdot, \neg, 0, 1)$ embedded into K
- K models actions, B propositions/state space

Kleene Algebras with Tests

algebraic semantics

while programs (without assignment):

$$\begin{aligned} \text{abort} &= 0 \\ \text{skip} &= 1 \\ x; y &= xy \\ \text{if } p \text{ then } x \text{ else } y &= px + \neg py \\ \text{while } p \text{ do } x &= (px)^* \neg p \end{aligned}$$

applications

- loop optimisation in while programs
- compiler optimisation
- encoding of propositional Hoare logic (see later)

Star-Continuous Kleene Algebras

$*$-continuous KAs

dioid with star axiom

$$xy^*z = \sum_{i \geq 0} (xy^i z)$$

intuition

star axiom is mixture of fixpoint iteration and continuity

facts

- every $*$-continuous KA is a KA
  (unfold and induction axioms are derivable)
- all KA models discussed are models of $*$-continuous KA
- equational theories of $*$-continuous KA and KA coincide

alternative

define KAs over quantales

Variants

KA axioms again

$$x + (y + z) = (x + y) + z \qquad x + y = y + x \qquad x + 0 = x \qquad x + x = x$$

$$x(yz) = (xy)z \qquad x1 = x \qquad 1x = x$$

$$x(y + z) = xy + xz \qquad (x + y)z = xz + yz$$

$$x0 = 0 \qquad 0x = 0$$

$$1 + xx^* \leq x \qquad z + xy \leq y \Rightarrow x^*z \leq y$$

$$1 + x^*x \leq x \qquad z + yx \leq y \Rightarrow zx^* \leq y$$

Variants

generalisations

- drop $x0 = 0$ interesting for general correctness semantics
- KAs over near-semirings: trace equivalence becomes bisimilarity
- KAs over pre-semirings: trace equivalence becomes simulation equivalence

expansions

- add $^\omega$-operation: ω-regular languages
- add $^\infty$-operation: refinement calculus/general correctness

homework

build your own variant!

Modal Kleene Algebras

- Part II -

Adding Modalities

[joint work with Jules Desharnais, Peter Jipsen, Szabolcs Mikulás]

motivation

- many applications require different approach to actions/propositions
- systems dynamics by state transitions $K \times B \to B$
- computational logics "use" KAs, but how precisely?

modal approach

- actions/propositions via Kripke frames
- modal operators via preimages/images $|x\rangle p \,/\, \langle x|p$
- preimages/images via axioms for domain/codomain

State Transitions

in KAT

"terminating program a from store p to store q" expressed as

$$pa \leq aq \quad \text{or equivalently} \quad pa\neg q = 0$$

proof of equivalence

$$pa = pa(q + \neg q) = paq + pa\neg q = paq + 0 \leq aq$$
$$pa\neg q \leq aq\neg q = a0 = 0$$

alternative

"q contains a-image of p"

question

how can we model images/preimages directly in idempotent semirings?

Adding Modalities

task

equational axioms for relational domain $d(x) = \{(p, p) : \exists q.(p, q) \in x\}$

approaches

1. domain as map $K \to B$
   [Desharnais/Möller/Struth ACM TOCL 2006]
2. domain as endo $S \to S$ that induces B
   [Desharnais/Struth SCP 2011]

Domain Semirings

domain semiring

semiring S with $d : S \to S$ that satisfies

$$x + d(x)x = d(x)x \qquad d(xy) = d(xd(y)) \qquad d(x+y) = d(x) + d(y)$$
$$d(x) + 1 = 1 \qquad d(0) = 0$$

lemma

domain semirings are dioids

proposition

$d^2 = d$ (domain is retraction), so $x \in d(S) \Leftrightarrow d(x) = x$

theorem

$(d(S), +, \cdot, 0, 1)$ is bounded DL (d induces state space)

Domain Algebra

proof

1. check closure properties, $d(1) = 1$ and $d(0) = 0$
2. this gives sub-semiring
3. $d(x) \leq 1$ is axiom and $d(x)d(x) = d(x)$
4. but semirings satisfying these two properties are distributive lattices [Birkhoff]

notation

- $(d(S), +, \cdot, 0, 1)$ is called domain algebra of S
- $p, q, r \ldots$ for domain elements

Domain Semirings

properties

- $d(x)x = x$ (domain is a left invariant)
- $x \leq d(y)x \Leftrightarrow d(x) \leq d(y)$ (domain is least left preserver)
- this is almost Galois connection
- many other natural properties hold
- range r axiomatised as domain on opposite semiring

modalities

$$|x\rangle y = d(xy) \qquad \langle x|y = r(yx)$$

yields distributive lattice with operators

Other Properties

let S be a domain semiring, let $x, y \in S$ and let $p \in d(S)$

- $d(x)x = x$ (domain is a left invariant)
- $d(p) = p$ (domain is a projection)
- $d(xy) \leq d(x)$ (domain increases for prefixes)
- $x \leq 1 \Rightarrow x \leq d(x)$ (domain expands subidentities)
- $d(x) = 0 \Leftrightarrow x = 0$ (domain is very strict)
- $d(1) = 1$ (domain is co-strict)
- $x \leq y \Rightarrow d(x) \leq d(y)$ (domain is isotone)
- $d(px) = pd(x)$ (domain elements can be exported)
- $d(x)d(x) = d(x)$ (domain elements are multiplicatively idempotent)
- $d(x)d(y) = d(y)d(x)$ (domain elements commute)
- $x \leq px \Leftrightarrow d(x) \leq p$ (domain elements are least left-preservers)
- $xy = 0 \Leftrightarrow xd(y) = 0$ (domain is weakly local)

Extension to Domain Semiring

proposition

semirings cannot always be extended to d-semirings

proof

consider $d(2)$ in dioid

$+$	0	1	2
0	0	1	2
1	1	1	1
2	2	1	2

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	0

1. $d(2) \neq 0$ since $d(x) = 0 \Leftrightarrow x = 0$
2. $d(2) \neq 1$ since otherwise $1 = d(2 \cdot d(2)) = d(2 \cdot 2) = d(0) = 0$
3. $d(2) \neq 2$ since otherwise $2 = d(2) \cdot 2 = 2 \cdot 2 = 0$

Domain Semirings

remark

- d-algebras need not be BAs (ex. 3-element S with $d(S)$ a chain)
- but $d(S)$ must contain maximal BA in $[0, 1]$
  - $x, y \in S$ with $x + y = 1$, $xy = 0 = yx$ form BA
  - and $d(x) = x$, $d(y) = y$

Antidomain Semirings

antidomain semiring

semiring S with map $' : S \to S$ that satisfies

$$x'x = 0 \qquad (xy)' \leq (xy'')' \qquad x'' + x' = 1$$

remarks

- domain definable via $d(x) = x''$ (Boolean complement)
- $d(S)$ induced is maximal BA in $[0, 1]$
- simple axioms induce rich modal calculus...
- axioms found with ATP system

Antidomain Semirings as Modal Semirings

diamonds again

$$|x\rangle y = d(xy) \qquad\qquad \langle x|y = r(yx)$$

consequence

very general way of defining modal logics

- we have $|x\rangle 0 = 0$ and $|x\rangle(p+q) = |x\rangle p + |x\rangle q$
- this yields BAOs

Modalities, Symmetries, Dualities

demodalisation

$$|x\rangle p \leq q \;\Leftrightarrow\; \neg q x p \leq 0 \qquad \langle x| p \leq q \;\Leftrightarrow\; p x \neg q \leq 0$$

dualities

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

symmetries

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

properties

- symmetries as theorem generators
- dualities as theorem transformers

Models

trace model

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

theorem

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

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

- subalgebras form trace MKAs

other models

- path, language, relation MKAs can again be obtained by forgetting
- in relation MKAs, sets are subidentities

MKA and PDL

theorem

MKAs are dynamic/test algebras [Trnkova/Reiterman,Nemeti,Pratt]

proof

(main task) show equivalence of

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

corollary

extensional MKAs are essentially propositional dynamic logics

$$(\forall p.|x\rangle p = |y\rangle p) \Rightarrow x = y \quad \text{(extensionality)}$$

MKA and PDL

a complex alternation theorem

$$p|x^*](\overset{x}{\rightarrow} q)(q \overset{x}{\rightarrow} p)) = |(xx)^*](p(q \overset{x}{\rightarrow} p)) \cdot |x(xx)^*](q(p \overset{x}{\rightarrow} q))$$

where $p \overset{x}{\rightarrow} q = p' + |x]q$

- 5-step Z3 proof in Isabelle
- $p = q$ yields Segerberg formula

MKA and LTL

encoding

- temporal operators (use one single action x)

$$Xp = |x\rangle p \qquad Fp = |x^*\rangle p \qquad Gp = |x^*]p \qquad pUq = |(px)^*\rangle q$$

- initial state $\mathsf{init}_x = [x|0$ "there's nothing before the beginning"
- validity of temporal implications $\sigma \models p \rightarrow q \Leftrightarrow \mathsf{init}_x p = q$

MKA and LTL

LTL axioms

von Karger's variant of [Manna/Pnueli]

$$|(px)^*\rangle q = q + p|x\rangle|(px)^*\rangle q \qquad \langle(xp)^*|q = q + p\langle(xp)^*|\langle x|q$$
$$|(px)^*\rangle 0 \leq 0 \qquad \langle x|0 = 1$$
$$|x^*](p \to q) \leq |x^*]p \to |x^*]q \qquad [x^*|(p \to q) \leq [x^*|p \to [x^*|q$$
$$|x^*]p \leq p|x]|x^*]p \qquad |x^*](p \to |x]p) \leq |x^*](p \to |x^*]p)$$
$$p \leq [x||x\rangle p \qquad p \leq |x]\langle x|p$$
$$\mathsf{init}_x \leq |x^*](p \to [x|q) \to |x^*](p \to [x^*|q) \qquad \mathsf{init}_x \leq |x^*]p \to |x^*][x|p$$
$$|x](p \to q) = |x]p \to |x]q \qquad [x|(p \to q) = [x|p \to [x|q$$
$$\langle x|p \leq [x|p \qquad |x\rangle p = |x]p$$

are theorems of MKA or express linearity of time in MKA

MKA and Hoare Logic

fact

MKA subsumes (propositional) Hoare logic

validity of Hoare triple

$$\models \{p\}x\{q\} \Leftrightarrow \langle x|p \leq q$$

example

validity of while rule $\langle x|pq \leq q \Rightarrow \langle (px)^*\neg p|q \leq \neg pq$

benefits

- wlp semantics for free ($\mathsf{wlp}(x,p) = |x]p$)
- soundness and completeness of Hoare logic easy in MKA
- Hoare logic deconstructed to equational modal reasoning

MKA and Hoare Logic

example

- validity of while-rule $\quad \langle x|\langle p|q \leq q \Rightarrow \langle (px)^*\neg p|q \leq \langle \neg p|q$
- proof

$$
\begin{aligned}
\langle x|\langle p|q \leq q &\Leftrightarrow \langle px|q \leq q && \text{(contravariance)}\\
&\Rightarrow \langle (px)^*|q \leq q && \text{(induction)}\\
&\Rightarrow \langle \neg p|\langle (px)^*|q \leq \langle \neg p|q && \text{(isotonicity)}\\
&\Leftrightarrow \langle (px^*)\neg p|q \leq \langle \neg p|q && \text{(contravariance)}
\end{aligned}
$$

Decidability of Hoare Logic

Hoare formulas

quasi-identities in modal Kleene algebra

$$\langle x_1 | p_1 \leq q_1, \ldots, \langle x_n | p_n \leq q_n \Rightarrow \langle a_0 | p_0 \leq q_0$$

PSPACE decision procedure

1. demodalisation: rewrite as equivalent quasi-identity in KAT

$$p_1 x_1 \neg q_1 \leq 0, \ldots, p_n x_n \neg q_n \leq 0 \Rightarrow p_0 x_0 \neg q_0 \leq 0$$

2. hypothesis elimination: reduce to equivalent identity $s' \leq t'$
3. apply PSPACE decision procedure for equational theory of KA(T)

Example: Termination Analysis

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

MKA K with divergence $^\nabla : K \to d(K)$ as greatest fixed point

$$x^\nabla \leq |x\rangle x^\nabla \qquad p \leq |x\rangle p + q \Rightarrow p \leq x^\nabla + |x^*\rangle q$$

encoding

- quasicommutation $yx \leq x(x+y)^*$
- separation of termination $(x+y)^\nabla = 0 \;\Leftrightarrow\; x^\nabla + y^\nabla = 0$

Example: Termination Analysis

result

extremely short proof reveals new refinement theorem

$$yx \leq x(x+y)^* \Rightarrow (x+y)^\nabla = x^\nabla + |x^*\rangle y^\nabla$$

proof

$$\begin{aligned}
(x+y)^\nabla &= y^\nabla + |y^*x\rangle(x+y)^\nabla \\
&\leq y^\nabla + |x(x+y)^*\rangle(x+y)^\nabla \\
&= y^\nabla + |x\rangle(x+y)^\nabla \\
&\leq x^\nabla + |x^*\rangle y^\nabla \\
&= 0 + |x^*\rangle 0 \\
&= 0
\end{aligned}$$

Example: Termination Analysis

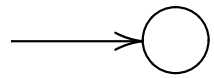
Backhouse Doornbos/van der Woude

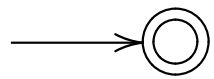
$$yx \leq x(x+y)^* + y \rightarrow (\nabla\ (x+y) = 0 \leftrightarrow \nabla\ x + \nabla\ y = 0)$$

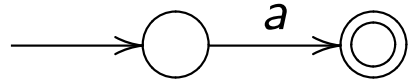
- 4-step Z3 proof in Isabelle
- original higher-order proof covers several pages

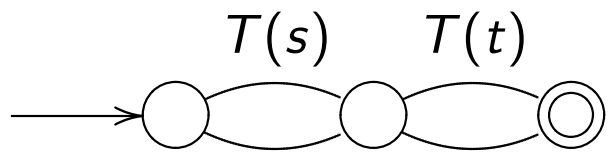
Domain Semirings and Andreka-Bredikhin Automata

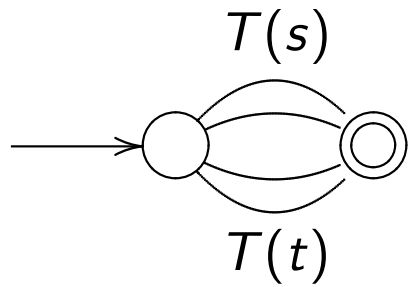
from d-semirings to automata

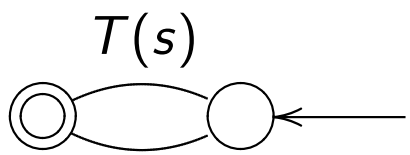
$T(0) =$ 

$T(1) =$ 

$T(a) =$ 

$T(s \cdot t) =$ 

$T(s \sqcap t) =$ 

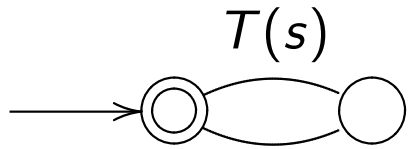
$T(s^\circ) =$ 

Domain Semirings and Andreka-Bredikhin Automata

for relations

$$d(x) = 1 \sqcap x \cdot x^{\circ}$$

domain automaton

$T(d(s)) =$ 

theorem

AB-automata under simulation (equivalence) form d-monoid

Domain Semirings and Andreka-Bredikhin Automata

distributivity laws

$$x(y+z) = xy + xz, \qquad (x+y)z = xz + yz, \qquad d(x+y) = d(x) + d(y)$$

polynomials

- every domain semiring term is equivalent to polynomial

$$m_0 + m_1 + \cdots + m_k$$

- every monomial can be written as trace

$$d(s_0)x_0 d(s_1)x_1 \ldots d(s_{n-1})x_{n-1} d(s_n)$$

because $d(x)d(y) = d(d(x)y)$ and $d(1) = 1$

Domain Semirings and Andreka-Bredikhin Automata

theorem

(sets of) AB-automata under simulation (equivalence) form d-monoid

- represent polynomial as set of monomials
- take downsets of associated atomata with respect to simulation preorder
- compare these sets

Free Domain Semirings

head normal form

domain term $d(xd(s_0)\dots d(s_n))$ and $d(s_i)$ also in hnf

fact

every domain term is equivalent to product of domain terms in hnf

completeness

for $T(s) \preceq T(t)$ we can show $t \leq s$

- assume terms in hnf, proceed by induction...

Representability

question

can one extend axiomatisations to characterise relational d-semirings?

theorem

[Andréka] for signature $\{+, \cdot\} \subseteq \Sigma \subseteq \{+, \cdot, 0, 1, ^*, ^\circ\}$, the class of representable Σ-algebras is not finitely axiomatisable

consequence

[Hirsch/Mikulás] the class of representable d/a-semirings is not finitely axiomatisable

Domain Semigroups

related work

- categories of partial maps
  (Carboni, Rosolini, Curien, Fiore, Cockett, . . .)
- functional domain semigroups
  (Bredikhin, Schein, Trokhimenko, Jackson/Stokes, . . .)
- relational domain semigroups
  (Hollenberg, Desharnais/Jipsen/Struth)

Concurrent Kleene Algebras

- Part III -

Concurrent Kleene Algebras

[joint work with CAR Hoare, P O'Hearn, B Möller, RL Petersen]

idea

add concurrent composition $||$ to KA

example

if $||$ is meet (parallelism à la product automata)

- then $(w||x);(y||z) \leq (w;y)||(x;z)$

example

if $||$ is shuffle (interleaving)

- then $(w||x);(y||z) \leq (w;y)||(x;z)$
- $(a||a);(b||b) = \{aabb\} < \{aabb, abab\} = (a;b)||(a;b)$

example

if $||$ is $+$ (disjoint concurrency)

- then $(w||x);(y||z) \geq (w;y)||(x;z)$

Concurrent Kleene Algebra

example

- let $(E, \rightarrow)$ be set of events with dependency relation $\rightarrow$
- for behaviours $X, Y \subseteq E$ write $X \not\leftarrow Y$ if nothing in X depends on anything in Y
- for systems $P, Q \subseteq 2^E$ define
  - fine-grained concurrency:
    $P * Q = \{X \cup Y : X \in P \wedge Y \in Q \wedge X \cap Y = \emptyset\}$
  - weak sequencing:
    $P; Q = \{X \cup Y : X \in P \wedge Y \in Q \wedge X \cap Y = \emptyset \wedge X \not\leftarrow Y\}$
  - disjoint concurrency:
    $P||Q = \{X \cup Y : X \in P \wedge Y \in Q \wedge X \cap Y = \emptyset \wedge X \not\leftarrow Y \wedge Y \not\leftarrow X\}$
- then

$$(P * Q); (R * S) \subseteq (P; R) * (Q; S)$$
$$(P||Q); (R||S) \supseteq (P; R)||(Q; S)$$

Concurrent Kleene Algebra

concurrent Kleene algebra

structure $(K, +, \cdot, ||, 0, 1, ^*, ^\star)$ where

- $(K, +, \cdot, 0, 1, ^*)$ is KA
- $(K, +, ||, 0, 1, ^\star)$ is commutative KA $(x||y = y||x)$
- exchange law $(w||x);(y||z) \leq (w;y)||(x;z)$ holds

remarks

- exchange law noticed by Bloom/Esik for shuffle languages
- used by Gischer for proving completeness result about pomsets
- equational exchange studied in relation algebra, Petri nets, ...
- called interchange law in 2-category theory

A Simple Model

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 (commutative) semigroup or monoid

independence relation

bilinear binary relation R on A

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

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 inner product, 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, S with $R \subseteq S$, and S symmetric

- $R(p+q, r) \wedge R(p, q) \Leftrightarrow R(q, r) \wedge R(p, q+r)$
- (small exchange)
  1. $R(p+q, r) \wedge S(p, q) \Rightarrow S(p, q+r) \wedge R(q, r)$
  2. $R(p, q+r) \wedge S(q, r) \Rightarrow S(p+q, r) \wedge R(p, q)$
- (exchange)
  $R(p+q, r+s) \wedge S(p, q) \wedge S(r, s) \Rightarrow R(p, r) \wedge R(q, s) \wedge S(p+r, q+s)$

Properties

proof

of exchange

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

Lifting

idea

understand system as set of possible aggregates

formalisation

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

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

example

for languages X, Y, word concatenation $+$ and universal relation R,
$\circ_R$ is language product

Lifting

extension

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

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

remarks

- lifting to dioid and Kleene algebra $(2^A,\cup,\circ_R,\emptyset,\{0\},^*)$ easy
- $X^* = \bigcup_{i\geq 0} X^i$
- commutative $(A,+)$ and R yields commutative algebras

Concurrent Monoids

extension

take structure/interaction of R, S into account

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

small exchange

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. $X \circ_R (Y \circ_S Z) \subseteq (X \circ_R Y) \circ_S Z$

exchange

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

$$(W \circ_S X) \circ_R (Y \circ_S Z) \subseteq (W \circ_R Y) \circ_S (X \circ_R Z)$$

Concurrent Monoids

concurrent semigroup

ordered bisemigroup $(S, \cdot, ||)$ that satisfies

$$x \cdot y \leq x||y, \qquad x||y = y||x,$$
$$(x||y) \cdot z \leq x||(y \cdot z), \qquad x \cdot (y||z) \leq (x \cdot y)||z,$$
$$(w||x) \cdot (y||z) \leq (w \cdot y)||(x \cdot z)$$

concurrent monoid

ordered bimonoid $(S, \cdot, ||, 1)$ that satisfies

$$x||y = y||x, \qquad (w||x) \cdot (y||z) \leq (w \cdot y)||(x \cdot z)$$

Concurrent Monoids

theorem

let $(A, +, 0)$ be commutative monoid, R, S bilinear, $R \subseteq S$ and S symmetric,

- $(2^A, \circ_R, \circ_S)$ is concurrent semigroup
- $(2^A, \circ_R, \circ_S, \{0\})$ is concurrent monoid if R, S also bistrict

remark

- this easily extends to concurrent dioids and Kleene algebras
- even to quantales

Sequential and Concurrent Compositions

aggregation algebra

distributive lattice $(A, +, \cdot, 0)$ with operator $f : A \to A$
(e.g. (pre)image operator on relational structure)

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

fact

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 order-dual exchange law holds

Hoare Calculus

Hoare triples

cheat: identify programs and assertions

$$\{x\}y\{z\} \Leftrightarrow x \cdot y \leq z$$

program y can extend every behaviour x to a behaviour in z

lemma

in ordered semigroup $(S, \cdot)$

- consequence: $x \leq x' \wedge \{x'\}y\{z'\} \wedge z' \leq z \Rightarrow \{x\}y\{z\}$
- composition: $\{x\}y\{w\} \wedge \{w\}y'\{z\} \Rightarrow \{x\}y \cdot y'\{z\}$
- skip: $\{x\}1\{x\}$ (in monoid)

all other Hoare rules (except assignment) derivable in CKA

Pomsets and Concurrent Semirings

pomsets

partially-ordered multisets are standard model of true concurrency

- they are partial orders $(S, \leq, \mu)$ with nodes labelled by symbols in Σ
- they generalise words (linear case) and multisets (empty order)

series parallel pomsets

built from atoms by two operations

- concurrent composition: $S||T = (S \cup T, \leq_S \cup \leq_T, \mu_S \cup \mu_T)$ if $S \cap T = \emptyset$
- series composition: $S \cdot T = (S \cup T, \leq_S \cup \leq_T \cup S \times T, \mu_S \cup \mu_T)$ if $S \cap T = \emptyset$

Pomsets and Concurrent Semirings

processes

sets of pomsets

operations

on processes

$$P||Q = \{S||T : S \in P \wedge T \in Q\}$$
$$P \circ Q = \{S \circ T : S \in P \wedge T \in Q\}$$

theorem

Pomsets and Concurrent Semirings

theorem

[Gischer] processes form free bimonoids/trioids (with $\|$ commutative)

subsumption

$S \prec T \;\Leftrightarrow\; \leq_S \supseteq \leq_T$ (S subsumed by T)

complex products

define operations on downward-closed sets of pomsets

theorem

[Gischer] the resulting algebras form free concurrent semirings

consequence

this yields decision procedure for concurrent semirings
(running time not yet analysed)

Towards Concurrent Separation Logic

- Part IV -

Algebra of Separation Logic

proposition

in ordered bisemigroup $(S, \cdot, || \leq)$ with $||$ commutative the following laws are equivalent:

- small exchange law $(x||y) \cdot z \leq x||(y \cdot z)$ and frame rule

$$\frac{\{x\}y\{z\}}{\{w||x\}y\{w||z\}}$$

- exchange law $(w||x) \cdot (y||z) \leq (w \cdot y)||(x \cdot z)$ and concurrency rule

$$\frac{\{x\}y\{z\} \wedge \{x'\}y'\{z'\}}{\{x||x'\}y||y'\{z||z'\}}$$

remark

these are rules of concurrent separation logic

Algebra of Separation Logic

problem

no shared unit in models of separation logic

resource model

- consider partial commutative monoid $(A, +, u)$ of functions under union if domains are disjoint
- for $X, Y \subseteq A$ define $X * Y = \{f + g : f \in X \wedge g \in Y\}$ and $1 = \{u\}$
- for predicate transformers $F_1, F_2 \in [2^A \to 2^A]$ define

$$(F_1 * F_2)X = \bigcup\{F_1X_1 * F_2X_2 : X_1 * X_2 \subseteq X\}$$

$$1X = X \cup 1 \qquad (F_1 \cdot F_2)X = F_1(F_2(X)) \qquad 1'X = X$$

theorem

- this forms concurrent monoid with two distinct units
- but frame rule (small exchange) fails

Locality

in resource model

transformer F is local if it can be described by action on parts of state

$$(F * 1')X = FX$$

in ordered bisemigroup

element x is local if $x * 1' = x$

theorem

in ordered bimonoid with $1' * 1' = 1'$ small exchange (i.e. frame rule) $(x * y) \cdot z \leq x * (y \cdot z)$ holds on concurrent submonoid of local y

consequence

only local elements should count as programs, non-local ones could be assertions

Conlusions

- Part V -

Research Questions

1. little is known about completeness/decidability of variants
2. free algebras for many variants are not known
3. study algebras from coalgebraic perspective (language derivatives)
4. relational respresentation theorems, finite axiomatisability of relational/language quasivarieties
5. nice algebras for ω-regular languages
6. spectrum of concurrency semantics for CKA
7. relationship CKA with linear logic
8. embed algebras into computational logic (dynamic, temporal, epistemic, separation)

Conclusion

- overview on variants of Kleene algebras
- sketch of mathematical techniques
- hint at applications
- structures are interesting as fundamental models of computation

- most imporant theorems and models implemented in interactive theorem prover Isabelle/HOL

`www.dcs.shef.ac.uk/~georg/isa`