Introduction to Separation Logic

Lectures at MGS'18

Georg Struth

on action short of strike at University of Sheffield, UK

Lecture 2: Assertion Algebra

This Lecture

- quantales
- assertion quantale of separation logic
- general convolution algebras
- intuitionistic assertions

Overview

- algebraic approach
- assertion quantale via construction of convolution algebra over PAM
- separating conjunction as convolution
- magic wand as its upper adjoint

Quantales

definition

- a quantale is structure $(Q, \leq, \cdot)$ where
  - $(Q, \leq)$ is complete lattice
  - $(Q, \cdot)$ is semigroup
  - $\cdot$ preserves sups in both arguments

$$x \cdot \bigsqcup_{i \in I} y_i = \bigsqcup_{i \in I} (x \cdot y_i) \qquad (\bigsqcup_{i \in I} x_i) \cdot y = \bigsqcup_{i \in I} (x_i \cdot y)$$

- a quantale is unital if its semigroup reduct is a monoid
- we write 0 for least element of Q and $\top$ for greatest element

we always consider unital quantales

Quantales

definition

- a quantale is abelian if the underlying monoid is
- it is distributive if $\sqcap$ preserves sups and $\sqcup$ preserves infs in both arguments
- a boolean quantale is a complemented distributive quantale
- we write $-x$ for the boolean complement of x

Residuation

definition

any quantale admits residuals

$$x\backslash z = \bigsqcup\{y \mid x \cdot y \leq z\} \qquad z/y = \bigsqcup\{x \mid y \cdot x \leq z\}$$

lemma

1. $x\backslash(-)$ and $(-)/y$ are upper adjoints of Galois connections

$$y \leq x\backslash z \Leftrightarrow x \cdot y \leq z \Leftrightarrow x \leq z/y$$

2. residuals coincide in abelian quantales

we will return to Galois connections in next lecture

Adjunction

proposition

every sup-preserving function between complete lattices has upper adjoint (more next lecture)

corollary

1. in distributive quantale, $\sqcap$ has relative pseudocomplement as residual

$$x \to z = \bigsqcup \{y \mid x \sqcap y \leq z\}$$

2. and pseudocomplement of x defined as $-x = x \to 0$
   - it is greatest y in quantale that satisfies $x \sqcap y = 0$
3. in boolean quantales, $x \to z = -x \sqcup z$ and $-x$ is boolean negation

Quantale of Booleans

example

- the booleans $\mathbb{B} = \{0, 1\}$ form quantale in which
  - $\cdot$ is $\sqcap$
  - $\backslash$ is boolean implication $\rightarrow$
- predicates over PAM S are boolean-valued functions of type $S \rightarrow \mathbb{B}$
- function spaces $\mathbb{B}^S$ and $\mathcal{P}\, S$ are isomorphic

Convolution Algebra

- we fix PAM $(S, \oplus, D, E)$ and abelian quantale $(Q, \leq, \cdot, 1)$
- we equip function space Q^S with quantale operations

Convolution Algebra

operations on Q^S

- composition $f, g : S \to Q$ is convolution

$$(f * g)\ x = \bigsqcup_{x = y \oplus z} f\ y \cdot g\ z$$

  - rhs is shorthand for $\bigsqcup\{w \mid \exists y, z.\ x = y \oplus z \wedge D\ y\ z \wedge w = f\ y \cdot g\ z\}$
- sups, infs and order are extended pointwise
  - $(\bigsqcup_{f \in F} f)\ x = \bigsqcup_{f \in F} f\ x$ and $(\bigsqcap_{f \in F} f)\ x = \bigsqcap_{f \in F} f\ x$
  - $f \leq g \Leftrightarrow \forall x.\ f\ x \leq g\ x$
- 0, 1 and $\top$ are lifted to functions $0 = \lambda x.\ 0$, $id = 1_E$, $\top = \lambda x.\ \top$
  - 1_E is indicator function for E (1 if $x \in E$, 0 otherwise)
  - for $E = \{1\}$ it reduces to Kronecker delta $\lambda x.\ \delta\ x\ 1$

Convolution Algebra

definition
$(Q^S, \leq, *, id)$ is convolution algebra over S and Q

theorem

1. if S is partial semigroup and Q quantale, then Q^S is quantale
2. if S is partial monoid and Q unital, then Q^S is unital
3. if S and Q are abelian, then so is Q^S
4. if Q is distributive, then so is Q^S
5. if Q is boolean, then so is Q^S

Convolution Algebra

lemma

if S is cancellative, then

$$(f * g)\, x = \bigsqcup_{y \preceq x} f\, y \cdot g\, (x \ominus y)$$

corollary

if X is set, then $Q^{X \times S}$ is unital quantale with

$$(f * g)\,(x, y) = \bigsqcup_{y = y_1 \oplus y_2} f\,(x, y_1) \cdot g\,(x, y_2) \qquad id\,(x, y) = \begin{cases} 1 & \text{if } y \in E \\ 0 & \text{otherwise} \end{cases}$$

Residuation in Convolution Algebra

observation

- $*$ has residual

$$f \multimap h = \bigsqcup \{g \mid f * g \leq h\}$$

- $f \multimap (-)$ is upper adjoint to $f * (-)$

theorem

if S is cancellative, then

$$(f \multimap g)\, x = \bigsqcap_{x = z \ominus y} f\, y \backslash g\, z$$

(rhs is shorthand for $\bigsqcap \{f\, y \backslash g\, z \mid y \preceq z \wedge x = z \ominus y\}$)

theorem links abstract definition of $\multimap$ with $\ominus$ in underlying PAM

Assertion Algebra of Separation Logic

instance

if $Q = \mathbb{B}$ then

- convolution on $\mathcal{P}(X \times S)$ is separating conjunction
- its residual is magic wand
- id is empty heap predicate emp

$$(f * g)(x, y) = \bigsqcup_{y = y_1 \oplus y_2} f(x, y_1) \sqcap g(x, y_2)$$

$$(f \mathrel{-\!\!*} g)(x, y) = \bigsqcap_{y = y_2 \ominus y_1} f(x, y_1) \to g(x, y_2)$$

$$id(x, y) = \delta\, y\, \varepsilon$$

corollary

$\mathcal{P}\, S_S$ is boolean abelian quantale of assertions over PAM S_S of statelets

Assertion Algebra of Separation Logic

separating conjunction

assertion $f * g$ holds of statelet (σ, η) if

- η can be split into heaplets η_1 and η_2
- f holds of (σ, η_1) and g holds of (σ, η_2)

as an algebraic operation, separating conjunction is not so idiosyncratic

Assertion Algebra of Separation Logic

magic wand

assertion $f \mathrel{-\!\!*} g$ holds of statelet (σ, η) if

- whenever η extends heaplet η_1 to heaplet η_2
- then g holds of (σ, η_2) if f holds of (σ, η_1)

alternatively

$f \mathrel{-\!\!*} g$ holds of $(\sigma, \eta_2 \ominus \eta_1)$ if

- whenever f holds of (σ, η_1)
- then g holds of (σ, η_2)

Assertion Algebra of Separation Logic

emp

- assertion emp holds of statelet (σ, η) if $\eta = \varepsilon$
- thus it holds of every unit statelet (σ, ε), for which heap is empty

infs and sups

- infs/sups correspond to universal/existential quantification over assertions ranging over S_S
- binary infs/sups express conjunctions/disjunctions

zero and top

- 0 corresponds to contradictory assertion over S_S
- $\top$ corresponds to valid assertion over S_S

Assertion Algebra of Separation Logic

summary

- assertions of separation logic are predicates over statelets
- they form boolean abelian quantales
  - separating conjunction is convolution
  - magic wand is its residual
- they were called bbi-algebras by Pym and O'Hearn
- we constructed them as instances of convolution algebras
  - this admits weighted assertions in quantales and even semirings
  - and non-abelian forms of convolution

Convolution in Context

every generalisation needs two instances!

Weighted Languages

$$(f * g)\, x = \sum_{x=y\cdot z} f\, y \cdot g\, z$$

- $f, g : \Sigma^* \to S$ are formal power series
- S is semiring, words are locally finite
- convolution algebra S^{Σ^*} forms semiring

language theory à la Schützenberger

Languages

$$(f * g)\, x = \sum_{x = y \cdot z} f\, y \sqcap g\, z$$

- $f, g : \Sigma^* \to \mathbb{B}$

convolution is language product

Matrices

$$(f * g)(i,j) = \bigsqcup_k f(i,k) \cdot g(k,j)$$

- $f, g : I \times I \to Q$
- $(i,j) = (i,k) \cdot (l,j) \wedge k = l$

convolution is matrix product

Relations

$$(f * g)(i,j) = \bigsqcup_k f(i,k) \cdot g(k,j)$$

- $f, g : I \times I \to \mathbb{B}$
- $(i,j) = (i,k) \cdot (l,j) \wedge k = l$

convolution is relational composition

Interval Temporal Logics

$$(f * g)(i,j) = \bigsqcup_k f(i,k) \cdot g(k,j)$$

- $f, g : P \times P \to \mathbb{B}$ for linear poset P
- $(i,j) = (i,k) \cdot (l,j) \wedge k = l$
- $f(i,j) = 0$ if $i \not\leq j$

convolution is chop modality

Incidence Algebras

$$(f * g)(i,j) = \bigsqcup_k f(i,k) \cdot g(k,j)$$

- $f, g : P \times P \to Q$ for poset P
- $(i,j) = (i,k) \cdot (l,j) \wedge k = l$
- $f(i,j) = 0$ if $i \not\leq j$

combinatorics à la Rota

Path Algebras

$$(f * g)\,\pi = \bigsqcup_{\pi = \pi_1 \oplus \pi_2} f\,\pi_1 \sqcap g\,\pi_2$$

- $f, g : P_G \to Q$ (with P_G set of finite paths in graph G)
- $\pi_1 \oplus \pi_2$ is path fusion

convolution is weighted product on paths

Trace Algebras

$$(f * g)\,\tau = \bigsqcup_{\tau = \tau_1 \oplus \tau_2} f\,\tau_1 \sqcap g\,\tau_2$$

- $f, g : T_G \to Q$ (with T_G set of finite traces in labelled graph G)
- $\tau_1 \oplus \tau_2$ is trace fusion

convolution is weighted product on traces

Lambek Calculus

$$(f * g)\, x = \bigsqcup_{R^x_{y\,z}} f\, y \sqcap g\, z$$

- $f, g : X \to \mathbb{B}$
- R^x_{yz} is ternary Kripke frame

convolution is binary product modality

Relational Convolution

$$(f *_R g)\, x = \bigsqcup_{R^x_{yz}} f\, y \cdot g\, z$$

- $f, g : X \to Q$
- $R \subseteq X \times X \times X$

Relational Convolution

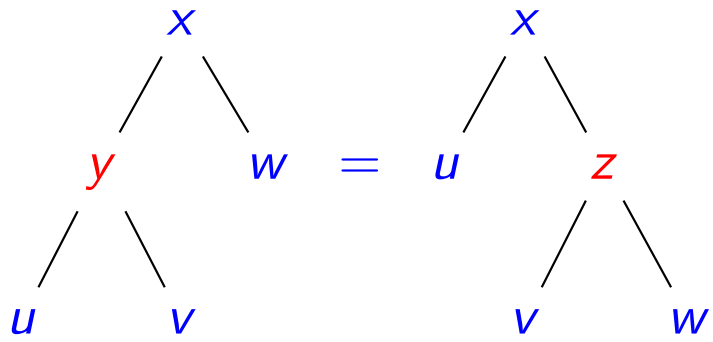
$$(f *_R g)\, x = \bigsqcup_{R^x_{yz}} f\, y \cdot g\, z$$

idea

- consider R^x_{yz} as (ternary) Kripke frame
- consider $*_R$ as (generalised) binary modality
- impose frame conditions on R to force properties of $*_R$

. . . like in modal correspondence theory of substructural logics

Associativity



lemma

$*_R$ is associative iff R is relationally associative:

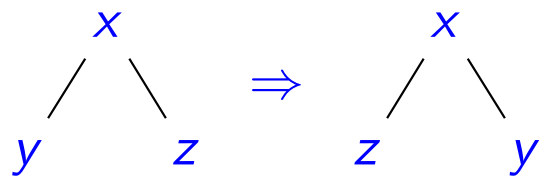
$$(f *_R g) *_R h = f *_R (g *_R h)$$

$$\Leftrightarrow$$

$$R^y_{uv} \wedge R^x_{yw} \Leftrightarrow R^x_{uz} \wedge R^z_{vw}$$

with "summation" over repeated indices

Commutativity



lemma

$*_R$ is commutative iff R is relationally commutative:

$$R^x_{yz} \Rightarrow R^x_{zy}$$

Units

lemma

the indicator function 1_{E_R}, $E_R \subseteq X$, is a unit of $*_R$ iff

$$\forall x \in X.\exists e \in E_R.\ R^x_{ex} \qquad \forall x \in X.\exists e \in E_R.\ R^x_{xe}$$

$$\forall x \in X.\forall e \in E_R.\ R^x_{ey} \Rightarrow x = y \qquad \forall x \in X.\forall e \in E_R.\ R^x_{ye} \Rightarrow x = y$$

Convolution Algebra

correspondence theorem

if Q is unital quantale, then (X, R) is relational monoid iff Q^X is unital quantale

context: complex duality

- categories of frames with bounded morphisms and
- categories of perfect BAOs with complete morphisms

lemma

every partial monoid $(S, \cdot, D, E)$ is r-semigroup with

$$R^x_{yz} \Leftrightarrow x = D\, y\, z \wedge y \cdot z$$

Relational Semigroups vs Hypersemigroups

hypersemigroup

structure $(X, \cdot)$ with $\cdot : X \to X \to \mathcal{P}\, X$ that satisfies

$$\{x\} \odot (y \cdot z) = (x \cdot y) \odot_s \{z\}$$

where $X \odot Y = \bigcup\{x \cdot y \mid x \in X \wedge y \in Y\}$

hypermonoid

h-semigroup with 1 such that $1 \cdot x = \{x\} = x \cdot 1$

remarks

- h-monoids are also called multimonoids or non-deterministic monoids
- they have been used in bbi-algebras by Galmiche/Larchey-Wendling
- and later by Brotherstone/Villard

Relational Semigroups vs Hypersemigroups

lemma

- relational semigroups and hypersemigroups are isomorphic

$$R^x_{y\,z} \Leftrightarrow x \in y \cdot z$$

- this extends to relational monoids with $E = \{1\}$ and hypermonoids

correspondence theorem

if Q is unital quantale, then X is h-semigroup iff Q^X is unital quantale with convolution

$$(f * g)\, x = \bigsqcup_{x \in y \cdot z} f\, y \| g\, z$$

Weighted Shuffle Algebras

shuffle of words

$\bowtie\colon X^* \to X^* \to \mathcal{P}\, X^*$ defined recursively

$$v \bowtie \varepsilon = \{v\} = \varepsilon \bowtie v$$
$$av \bowtie bw = \{a\} \cdot (v \bowtie bw) \cup \{b\} \cdot (av \bowtie w)$$

lemma

$(X^*, \bowtie, \varepsilon)$ is abelian h-monoid

corollary

if Q is abelian unital quantale, then so is Q^{X^*} and

$$(f * g)\, x = \bigsqcup_{x \in y \bowtie z} f\, y \| g\, z$$

Convolution Algebra

- construction recipe for convolution algebras over relational monoids
- links with modal correspondence/duality theory
- assertion quantale of separation logic is just an instance out of many
- separating conjunction is just an instance of convolution

Intuitionistic Assertions

definition

predicate p is intuitionistic if $(\sigma, \eta_1) \in p \wedge \eta_1 \subseteq \eta_2 \Rightarrow (\sigma, \eta_2) \in p$

lemma

for PAM S and $p \in \mathcal{P}\, S$, the following are equivalent

1. p is intuitionistic
2. p is isotone: $x \preceq y \Rightarrow p\, x \leq p\, y$ for all $x, y \in S$
3. $\top * p \leq p$, in fact, $\top * p = p$
4. $p \leq \top \mathrel{-\!\!*} p$, in fact, $p = \top \mathrel{-\!\!*} p$.

being intuitionistic relates to adjoints $\top \cdot (-)$ and $\top \backslash (-)$ in quantale

Quantic Nuclei and Co-Nuclei

definition

- element p of quantale Q is left-sided if it is a fixpoint of $\nu = \top \cdot (-)$ (equivalently of $\nu^\natural = \top \backslash (-)$)
- $\nu[Q] = \nu^\natural[Q]$ denotes set of left-sided elements in Q
- left-sided $=$ intuitionistic

definition

- a quantic nucleus of Q is a closure operator $f : Q \to Q$ that satisfies

$$(f\,x) \cdot (f\,y) \leq f\,(x \cdot y)$$

- a quantic conucleus of Q is a coclosure operator $f : Q \to Q$ that satisfies the above lax identity

Quantic Nuclei and Co-Nuclei

theorem [Niefield/Rosenthal]

1. if $f : Q \to Q$ is nucleus, then
   - $f[Q]$ is quantale with composition $f((-) \cdot (-))$ and sup $f(\bigsqcup(-))$
   - $f : Q \to f[Q]$ is quantale morphism that preserves composition and non-empty sups
2. if $g : Q \to Q$ is conucleus, then
   - $g[Q]$ is a subalgebra of Q
   - $g : g[Q] \to Q$ is embedding that preserves composition and sups except for $\top$

we don't expect that quantale morphisms preserve units

Intuitionistic Elements

lemma

- $\nu^\natural$ is conucleus on any quantale
- ν is nucleus on any abelian quantale

lemma

$\nu : \nu^\natural[Q] \to \nu[Q]$ and $\nu^\natural : \nu[Q] \to \nu^\natural[Q]$ form bijective pair of inf-preserving quantale morphisms

theorem

1. $\nu[Q]$ is subquantale of Q (without unit) that is isomorphic to $\nu^\natural[Q]$; $\nu^\natural$ and ν preserve infs in Q and $\nu[Q]$ as well as 0 and $\top$
2. if Q is abelian, then so is $\nu[Q]$, and ν and $\nu^\natural$ preserve $\setminus$ ($\twoheadrightarrow$) in $\nu[Q]$
3. if Q is boolean, then $\nu^\natural[Q]$ is distributive subquantale (without unit) that is relatively pseudocomplemented by $\nu^\natural(p \to q)$

Intuitionistic Elements

consequence

intuitionistic elements of boolean quantales form Heyting algebras with

$$\nu^\natural\,(p \to q) = \bigsqcup\{r \mid p \sqcap r \leq q \wedge r \in \nu[Q]\}$$

theorem

$\nu^\natural[Q] \models p \leq q \Leftrightarrow Q \models \nu^\natural\, p \leq \nu^\natural\, q$ holds in every boolean quantale Q

remarks

- this generalises Ishtiaq/O'Hearn's Gödel translation from intuionistic to classical predicates in separation logic
- results hold in arbitrary boolean quantales
- most constructions seem to generalise to residuated lattices

Summary

- assertion quantale of separation logic obtained as convolution algebra
- algebraically speaking, separating conjunction is not so special
- intuitionistic assertions related with (co)nuclei—a standard concept from quantales

next lecture: predicate transformer semantics for separation logic

Exercises

?

Further Reading

- Brotherstone, Villard, *Sub-Classical Boolean Bunched Logics and the Meaning of Par*
- Calcagno et al, *Local Action and Abstract Separation Logic*
- Dongol, Gomes, Struth, *A Program Construction and Verification Tool for Separation Logic*
- Dongol, Hayes, Struth, *Convolution as a Unifying Concept*
- Dongol, Hayes, Struth, *Relational Convolution, Generalised Modalities and Incidence Algebras*
- Galmiche, Larchey-Wendling, *Non-Deterministic Phase Semantics and the Undecidability of Boolean BI*
- Ishtiaq, O'Hearn, *BI as an Assertion Language for Mutable Data Structures*
- Niefield, Rosenthal, *Constructing Locales from Quantales*
- O'Hearn, Pym, *The Logic of Bunched Implications*
- Reynolds, *Separation Logic: A Logic for Shared Mutable Data Structures*
- Rosenthal, *Quantales and Their Applications*
- Isabelle components: https://www.isa-afp.org/entries/PSemigroupsConvolution.html