Situated reasoner

Naso Evangelou-Oost (Oneironaut)

6 June 2023

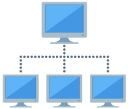
The University of Queensland
Australia

Introduction

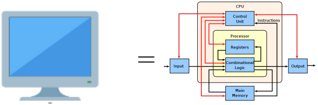
- Concurrent & distributed systems are everywhere, yet really hard to reason about.
- Compositional methods mitigate the combinatorial explosion of possibilities when many interacting systems combine.
- Concurrent valuation algebras (CVAs) are. . .
    - compositional, modular, local,
    - algebraic, lattice-based,
    - able to detect subtle information inconsistency (e.g. sequential inconsistency),
    - algorithmically tractable.

Topologies encode the connective structure of distributed and concurrent systems:

- Topology $\mathscr{T}$ for distributed systems: networks.



- Topology $\mathscr{T}$ for concurrent systems: shared memory and resources.



A ***presheaf*** is a contravariant functor on a topology $\mathscr{T}$

$$\Phi : \mathscr{T}^{op} \to \mathscr{P}os$$

I.e. we have,

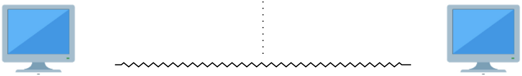
- ***Object map***: A function sending each domain $A \in \mathscr{T}$ to a poset Φ_A.
- ***Arrow map***: A function sending each inclusion $B \subseteq A$ to a monotone ***restriction map*** $a \mapsto a^{\downarrow B} : \Phi_A \to \Phi_B$.
- ***Transitivity***: For $C \subseteq B \subseteq A$ and $a \in \Phi_A$,

$$(a^{\downarrow B})^{\downarrow C} = a^{\downarrow C}$$

- ***Identity law***: For each $A \in \mathscr{T}$ and $a \in \Phi_A$,

$$a^{\downarrow A} = a$$

$$
\begin{tikzcd}
 & \Phi_{A\cup B} \arrow[dl] \arrow[dr] & \\
\Phi_A \arrow[dr, "a \mapsto a^{\downarrow A\cap B}"'] & & \Phi_B \arrow[dl, "b \mapsto b^{\downarrow A\cap B}"] \\
 & \Phi_{A\cap B} &
\end{tikzcd}
$$



(covariant) Grothendieck construction

Given $\Phi : \mathcal{T}^{op} \to \mathcal{P}os$, combine all the posets Φ_A into one big poset $\int \Phi$.

$$\int \Phi = \{(A, a) \mid A \in \mathcal{T}, a \in \Phi_A\}$$

Partial order $\preceq$:

$$(A, a) \preceq (B, b) \iff B \subseteq A \text{ and } a^{\downarrow B} \leq_{\Phi_B} b$$

Shorthand: write a instead of (A, a) leaving domain implicit; use ***domain*** map d to recover domain

$$\mathrm{d} : \int \Phi \to \mathcal{T}^{op}$$
$$\mathrm{d}a = \text{domain of } a$$

Ordered valuation algebras (OVAs)

Definition. An ***ordered valuation algebra (OVA)*** consists of...

- a poset-valued presheaf
$$\Phi : \mathcal{T}^{op} \to \mathcal{P}os$$
- a binary operator
$$\otimes : \int \Phi \times \int \Phi \to \int \Phi$$
- a natural transformation
$$\epsilon : 1 \Rightarrow \Phi$$
(i.e. an element $\epsilon_A \in \Phi_A$ for each A such that $\epsilon_A^{\downarrow B} = \epsilon_B$ whenever $B \subseteq A$.)

Obeying the following axioms...

- ***Ordered semigroup***:
$$\otimes \text{ is associative and monotone}$$
- ***Labelling***:
$$\mathrm{d}(a \otimes b) = \mathrm{d}a \cup \mathrm{d}b$$
- ***Neutrality***:
$$\epsilon_{\mathrm{d}a} \otimes a = a = a \otimes \epsilon_{\mathrm{d}a}$$
- ***Combination***:
$$(a \otimes b)^{\downarrow \mathrm{d}a} = a \otimes b^{\downarrow \mathrm{d}a \cap \mathrm{d}b} \text{ and } (a \otimes b)^{\downarrow \mathrm{d}b} = a^{\downarrow \mathrm{d}a \cap \mathrm{d}b} \otimes b$$

Extension

Theorem. Let $(\Phi, \otimes, \epsilon)$ be an OVA. For each inclusion $B \subseteq A$ in $\mathcal{T}$, there is an adjunction

$$a^{\downarrow B} \leq_{\Phi_B} b \iff a \leq_{\Phi_A} \epsilon_a \otimes b$$

We call $b \mapsto \epsilon_a \otimes b$ ***extension of b to A*** and write $b^{\uparrow A} := \epsilon_a \otimes b$.

Some facts:

- Extension is a functor: if $C \subseteq B \subseteq A$ and $c \in \Phi_C$, then
$$(c^{\uparrow B})^{\uparrow A} = c^{\uparrow A} \text{ and } c^{\uparrow C} = c$$
- If Φ has the ***strongly neutral property:*** $\forall A, B \in \mathcal{T}$ ***we have*** $\epsilon_A \otimes \epsilon_B = \epsilon_{A \cup B}$, then for all $B \subseteq A$,
$$\epsilon_B^{\uparrow A} = \epsilon_A$$
- Restriction after extension is the identity map, i.e., for $B \subseteq A$ and $b \in \Phi_B$,
$$(b^{\uparrow A})^{\downarrow B} = b$$
- Extension after restriction is a ***closure operator***, i.e., for $B \subseteq A$ and $a \in \Phi_A$,
$$a \leq_{\Phi_A} (a^{\downarrow B})^{\uparrow A} \qquad \text{and} \qquad (((a^{\downarrow B})^{\uparrow A})^{\downarrow B})^{\uparrow A} = (a^{\downarrow B})^{\uparrow A}$$
- If for each $A \in \mathcal{A}$, Φ_A is a complete lattice, then so is $\int \Phi$.

Definition. A ***concurrent valuation algebra (CVA)*** consists of...

- A commutative OVA
$$(\Phi, \parallel, \delta)$$
- A (generally noncommutative) OVA
$$(\Phi, \fatsemi, \epsilon)$$

Obeying the following axioms...

- ***Weak exchange***:
$$(a \parallel b) \fatsemi (c \parallel d) \preceq (a \fatsemi c) \parallel (b \fatsemi d)$$
- ***Neutral laws***:
$$\epsilon_A \preceq \epsilon_A \parallel \epsilon_A \text{ and } \delta_A \fatsemi \delta_A \preceq \delta_A$$

- ***Refinement***:

$$a \preceq b \iff \mathrm{d}b \subseteq \mathrm{d}a \text{ and } a^{\downarrow \mathrm{d}b} \leq_{\Phi_{\mathrm{d}b}} b$$

- ***Hoare triple (Hoare logic)***:

$$p \ \{a\} \ q := p \mathbin{;} a \preceq q$$

- ***Jones quintuple (rely-guarantee logic)***:

$$p \ r \ \{a\} \ g \ q := p \ \{a \parallel r\} \ q \text{ and } a \preceq g$$ [1]

[1] Ian doesn't like this.

Trace models

- Trace models: specifications are subsets of ***traces*** = lists of observations $t = [t_1, \ldots, t_n]$.
- Can be coupled to a clock or not. What does the i in t_i mean?
- Decoupling from a global clock = stuttering invariance (traces of states);

$$[1, 1, 2, 3, 3, 3] \sim [1, 2, 2, 3]$$

Two ways to encode stuttering-invarance:

- Stuttering closure: if the first trace belongs to a specification, so does the second.
- Stuttering reduction: both traces are identified in a quotient.

Parallel and sequential

Depends on what the elements t_i in a trace $t = [t_1, \ldots, t_n]$ mean:

- ***State***: t_i is a state of the system.
  - Parallel = sync = $\wedge_A = \cap$,
  $$\{[a, b, c]\} \wedge_A \{[a, b, c]\} = \{[a, b, c]\}$$
  - Sequential = gluing concatenation = $\smile$.
  $$\{[a, b, c]\} \smile_A \{[c, d]\} = \{[a, b, c, d]\}$$
- ***Action***: t_i is an action taken by the system.
  - Parallel = shuffle = $\sqcup\!\sqcup$,
  $$\{[a, b, c]\} \sqcup\!\sqcup_A \{[d, e]\} = \{[a, b, d, e, c], [d, a, b, c, e], [a, b, d, c, e], \ldots\}$$
  - Sequential = concatenation = $\frown$,
  $$\{[a, b, c]\} \frown_A \{[d, e]\} = \{[a, b, c, d, e]\}$$

State trace CVA Σ

- State functor: $\Omega_A^{\text{state}} := A \to \mathbb{Z}$ (A-tuples)
- Nonempty list functor: $L_+ : \mathcal{S}et \to \mathcal{S}et$
- Powerset functor: $P : \mathcal{S}et \to \mathcal{P}os$

State trace CVA Σ is defined as the composite,

$$\Sigma = \ \mathcal{T}^{op} \xrightarrow{\Omega^{\text{state}}} \mathcal{S}et \xrightarrow{L_+} \mathcal{S}et \xrightarrow{P} \mathcal{P}os$$

- Parallel = synchronisation = meet:

$$\wedge : \textstyle\int \Sigma \times \int \Sigma \to \int \Sigma$$

$$a \wedge b := a^{\uparrow \mathrm{d}a \cup \mathrm{d}b} \cap b^{\uparrow \mathrm{d}a \cup \mathrm{d}b}$$

- Sequential = gluing concatenation, matches final/initial states:

$$\smile : \textstyle\int \Sigma \times \int \Sigma \to \int \Sigma$$

$$a \smile b := a^{\uparrow \mathrm{d}a \cup \mathrm{d}b} \smile_{\mathrm{d}a \cup \mathrm{d}b} b^{\uparrow \mathrm{d}a \cup \mathrm{d}b}$$

- Neutral elements for parallel, sequential resp.

$$\top : 1 \Rightarrow \Sigma \qquad\qquad \nu : 1 \Rightarrow \Sigma$$

$$\top_A = L_+(\Omega_A^{\text{state}}) \qquad\qquad \nu_A = \left\{ t \in L_+(\Omega_A^{\text{state}}) \mid \lambda(t) = 1 \right\}$$

- Action functor: $\Omega^{\text{act}} : \mathcal{T}^{op} \to \mathcal{S}et$
  - $\Omega^{\text{act}}_A = \mathbb{Z}^A \times \mathbb{Z}^A$ (events = pairs of states)
  - $\Omega^{\text{act}}_A = P(\mathbb{Z}^A \times \mathbb{Z}^)$ (events with external choice)
  - $\Omega^{\text{act}}_A = A \times A \to \mathbb{Z}$ (linear functions $\mathbb{Z}^A \to \mathbb{Z}^A$)

Action trace CVA Γ is defined as the composite:

$$\Gamma = \ \mathcal{T}^{op} \xrightarrow{\Omega^{\text{act}}} \mathcal{S}et \xrightarrow{L} \mathcal{S}et \xrightarrow{P} \mathcal{P}os$$

- Parallel = shuffle:

$$\sqcup\!\sqcup : \textstyle\int \Gamma \times \int \Gamma \to \int \Gamma$$
$$a \sqcup\!\sqcup b := a^{\uparrow \mathrm{d}a \cup \mathrm{d}b} \sqcup\!\sqcup_{\mathrm{d}a \cup \mathrm{d}b} b^{\uparrow \mathrm{d}a \cup \mathrm{d}b}$$

- Sequential = concatenation:

$$\frown : \textstyle\int \Gamma \times \int \Gamma \to \int \Gamma$$
$$a \frown b := a^{\uparrow \mathrm{d}a \cup \mathrm{d}b} \frown_{\mathrm{d}a \cup \mathrm{d}b} b^{\uparrow \mathrm{d}a \cup \mathrm{d}b}$$

- Neutral element (same for $\sqcup\!\sqcup$ and $\frown$):

$$\iota : 1 \Rightarrow \Gamma$$
$$\iota_A = \{[\,]_A\}$$

- ***Free semigroup with idempotent generators*** $I : \mathcal{S}et \to \mathcal{S}emi$
  $I(S) = L_+(S)$ modulo $ss \sim s$ for all $s \in S$, with concatenation as multiplication.

Relative state trace CVA Σ^{rel} is defined as the composite:

$$\Sigma^{\text{rel}} = \mathcal{T}^{op} \xrightarrow{\Omega^{\text{state}}} \mathcal{S}et \xrightarrow{I} \mathcal{S}emi \xrightarrow{U} \mathcal{S}et \xrightarrow{P} \mathcal{P}os$$

Combine operators and neutral elements defined as in Σ.

- Projection and parallel no longer preserve the length of traces.
  Parallel syncs on common variables, shuffles on disjoint variables. E.g. $a, b \in \int \Sigma^{\text{rel}}$ with $\mathrm{d}a = \{x, y\}$ and $\mathrm{d}b = \{y, z\}$,

$$a \wedge^{\text{rel}} b = \left\{ \begin{bmatrix} x_0 & x_1 & x_1 \\ y_0 & y_0 & y_1 \end{bmatrix} \right\} \wedge \left\{ \begin{bmatrix} y_0 & y_0 & y_1 \\ z_0 & z_1 & z_1 \end{bmatrix} \right\}$$

$$= \left\{ \begin{bmatrix} x_0 & x_1 & x_1 \\ y_0 & y_0 & y_1 \\ z_0 & z_1 & z_1 \end{bmatrix}, \begin{bmatrix} x_0 & x_1 & x_1 & x_1 \\ y_0 & y_0 & y_0 & y_1 \\ z_0 & z_0 & z_1 & z_1 \end{bmatrix}, \begin{bmatrix} x_0 & x_0 & x_1 & x_1 \\ y_0 & y_0 & y_0 & y_1 \\ z_0 & z_1 & z_1 & z_1 \end{bmatrix} \right\}$$

Morphisms of OVAs & CVAs

Definition. A ***lax morphism of OVAs*** $f : (\Phi, \otimes, \epsilon) \to (\Phi', \otimes', \epsilon')$ is a family of maps $\{f_A : \Phi_A \to \Phi'_A\}_{A \in \mathcal{T}}$, obeying for all $a \in \Phi_A$, $b \in \Phi_B$ and $C \subseteq A$...

- ***Monotonicity***:
$$a \preceq b \implies f_A(a) \preceq f_B(b)$$
- ***Lax naturality***:
$$f_A(a)^{\downarrow C} \preceq f_C(a^{\downarrow C})$$
- ***Lax multiplicativity.***
$$f_A(a) \otimes' f_B(b) \preceq f_{A \cup B}(a \otimes b)$$
- ***Lax unitality.***
$$\epsilon'_A \preceq f_A(\epsilon_A)$$

Definition. A ***lax morphism of CVAs*** $f : (\Phi, \|, \delta, \fatsemi, \epsilon) \to (\Phi', \|', \delta', \fatsemi', \epsilon')$ is a map f that is both...

- a lax morphism of (commutative) OVAs $(\Phi, \|, \delta) \to (\Phi', \|', \delta)$,
- a lax morphism of OVAs $(\Phi, \fatsemi, \epsilon) \to (\Phi', \fatsemi', \epsilon)$.

Reversing the inequalities above defines a ***colax morphism***.

Colax morphism from Σ to Σ^{rel}

Notice $L_+ \cong U \circ F$ where ***F is the free semigroup functor***.
For each set X there is a quotient map $q_X : F(X) \twoheadrightarrow I(X) \cong F(X)/\sim$ where $\sim$ is the congruence generated by $x = xx$ for all $x \in X$. This map does a ***stuttering reduction***.
This is natural in X, so we get a natural transformation $q : F \Rightarrow I$.
By composing (whiskering), this gives a natural transformation $f : \Sigma \Rightarrow \Sigma^{\mathrm{rel}}$.

$$f = \begin{tikzcd} \mathcal{T}^{op} \arrow[r, "\Omega^{\mathrm{state}}"] & \mathcal{S}et \arrow[r, bend left, "F"] \arrow[r, bend right, "I"'] \arrow[r, phantom, "\Downarrow q"] & \mathcal{S}emi \arrow[r, "U"] & \mathcal{S}et \arrow[r, "P"] & \mathcal{P}os \end{tikzcd}$$

Moreover, f is a colax morphism of CVAs:

- $a \preceq b \implies f(a) \preceq f(b)$
- $f(\top) \preceq \top^{\mathrm{rel}}$
- $f(\nu) \preceq \nu^{\mathrm{rel}}$
- $f(a \wedge b) \preceq f(a) \wedge^{\mathrm{rel}} f(b)$ (note this is not equality: consider $a = [xx]$ and $b = [x]$.)
- $f(a \smile b) \preceq f(a) \smile^{\mathrm{rel}} f(b)$

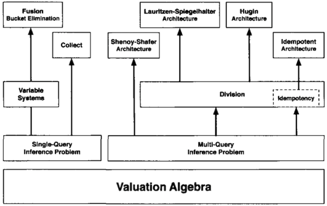
There should be a right-adjoint $g : \Sigma^{\mathrm{rel}} \to \Sigma$ that does stuttering closure...

Local computation

Efficient computation is enabled by the ***combination*** law:

$$(a \otimes b)^{\downarrow \mathrm{d}a} = a \otimes b^{\downarrow \mathrm{d}a \cap \mathrm{d}b}$$
$$(a \otimes b)^{\downarrow \mathrm{d}b} = a^{\downarrow \mathrm{d}a \cap \mathrm{d}b} \otimes b$$

The LHS is usually ***expensive*** to compute, but the RHS can be ***much cheaper*** if $\mathrm{d}a \cap \mathrm{d}b$ is small.



- Local computation framweork specialises to standard optimal algorithms in databases, probabilistic graphical models, CSPs, dynamic programming, ...
- We can already use these algorithms in a CVA on just parallel combinations.
- Need to generalise to noncommutative case & with 2 combine operators.
- Theoretically feasible from the generalised combination rule, but not yet implemented.

Summary & future work

Summary:

- We introduced CVAs, a modular/local/compositional algebra for specifying concurrent/distributed systems.
- CVAs support a duoidal parallel/sequential algebraic structure, refinement, Hoare and rely-guarantee logics.
- We described 3 example trace models of CVAs and related them by morphisms.
- CVAs have a path to efficient algorithms for inference, static analysis, model checking...

Future work:

- More models: Aczel trace models, graph models, sheaf based models that better capture local properties...
- Push-forward/pullback of OVAs/CVAs on different spaces.
- Develop local computation algorithms.
- Formalisation in Isabelle.

References:

Evangelou-Oost, Nasos, Callum Bannister and Ian J. Hayes (2023). 'Contextuality in Distributed Systems'. In: ***Relational and Algebraic Methods in Computer Science***. Springer International Publishing, pp. 52–68.

Evangelou-Oost, Nasos, Callum Bannister, Larissa Meinicke et al. (2023). ***Trace models of concurrent valuation algebras***. arXiv: 2305.18017 [cs.LO].

Contact: naso@oneironaut.dev, linkedin.com/in/nasosev

THANK YOU!