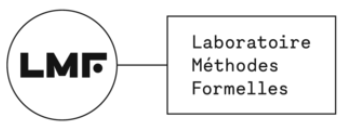
Specification Theories, Reloaded Relationally

Uli Fahrenberg Paul Brunet

LMF, Université Paris-Saclay

LACL, Université Paris-Est Créteil

RAMiCS, April 2026



Motivation

Not so easy...

Motivation

Not so easy...

Incremental certification / Compositional verification

- bottom-up and top-down

Wish list:

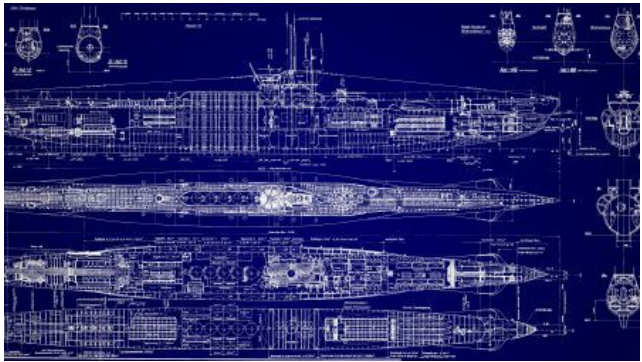
- $\mathsf{Mod} \vDash \mathsf{Spec}_1 \;\&\; \mathsf{Spec}_1 \leq \mathsf{Spec}_2 \implies \mathsf{Mod} \vDash \mathsf{Spec}_2$
- $\mathsf{Mod} \vDash \mathsf{Spec}_1 \;\&\; \mathsf{Mod} \vDash \mathsf{Spec}_2 \implies \mathsf{Mod} \vDash \mathsf{Spec}_1 \wedge \mathsf{Spec}_2$
- $\mathsf{Mod}_1 \vDash \mathsf{Spec}_1 \;\&\; \mathsf{Mod}_2 \vDash \mathsf{Spec}_2 \implies \mathsf{Mod}_1 \parallel \mathsf{Mod}_2 \vDash \mathsf{Spec}_1 \parallel \mathsf{Spec}_2$
- $\mathsf{Mod}_1 \vDash \mathsf{Spec}_1 \;\&\; \mathsf{Mod}_2 \vDash \mathsf{Spec} \,/\, \mathsf{Spec}_1 \implies \mathsf{Mod}_1 \parallel \mathsf{Mod}_2 \vDash \mathsf{Spec}$

Compositional Verification

- $\mathsf{Mod} \vDash \mathsf{Spec}_1$ & $\mathsf{Spec}_1 \leq \mathsf{Spec}_2 \implies \mathsf{Mod} \vDash \mathsf{Spec}_2$
  - incrementality
- $\mathsf{Mod} \vDash \mathsf{Spec}_1$ & $\mathsf{Mod} \vDash \mathsf{Spec}_2 \implies \mathsf{Mod} \vDash \mathsf{Spec}_1 \wedge \mathsf{Spec}_2$
  - conjunction
- $\mathsf{Mod}_1 \vDash \mathsf{Spec}_1$ & $\mathsf{Mod}_2 \vDash \mathsf{Spec}_2 \implies \mathsf{Mod}_1 \parallel \mathsf{Mod}_2 \vDash \mathsf{Spec}_1 \parallel \mathsf{Spec}_2$
  - compositionality
- $\mathsf{Mod}_1 \vDash \mathsf{Spec}_1$ & $\mathsf{Mod}_2 \vDash \mathsf{Spec} \,/\, \mathsf{Spec}_1 \implies \mathsf{Mod}_1 \parallel \mathsf{Mod}_2 \vDash \mathsf{Spec}$
  - quotient

Not so easy – but easier than model checking?

Application? Naval Group



- thousands of components; computing, physical, and mixed; from hundreds of subcontractors
- modern design needs formal(ish) verification
- what if between verification and implementation, a subcontractor decides to improve a component??

Today

What precisely is a specification theory?

- [Pnueli '85], [Hennessy-Milner '85], [Larsen '90]
- [Aceto et al '19], [Beneš et al '20], [F.-Legay '20], [F.-Legay '21], [F. '22]
- Still not clear!
- Useful to work out for developing quantitative versions, for example
- Back to basics, using a relational setting

Specification Formalisms

Definition

A specification formalism is a structure $(M, S, \vDash)$ with a satisfaction relation $\vDash$: $M \multimap S$ between a set M of models and a set S of specifications / formulas.

- Induces preorders and equivalences:

$$\sqsubseteq := \vDash \,/\, \vDash \qquad\qquad \preceq := \vDash \setminus \vDash$$
$$\sqsupseteq := \sqsubseteq \cap \sqsupseteq \qquad\qquad \simeq := \preceq \cap \succeq$$

Lemma

For $m_1, m_2 \in M$, $m_1 \sqsubseteq m_2$ iff $m_2 \vDash s \implies m_1 \vDash s$ for all $s \in S$.

Lemma

For $s_1, s_2 \in S$, $s_1 \preceq s_2$ iff $m \vDash s_1 \implies m \vDash s_2$ for all $m \in M$.

- $\sqsupseteq$ is Hennessy-Milner behavioral equivalence
- $\simeq$ is semantic equivalence of logical formulas

Characteristic Formulas

Definition

$s \in S$ is characteristic for $m \in M$, denoted $m \vdash s$, if

$$\forall m' \in M : m' \vDash s \iff m' \sqsubseteq m.$$

- so $\vdash \;\leftrightarrow\; \vDash \cap (\sqsubseteq / \dashv)$
- and $\dashv ; \vdash \;\rightarrow\!\!\!\!\!\rightarrow\; \simeq$, *i.e.*, $\vdash$ is a partial function up-to $\simeq$ (as expected)

Expressive Specification Formalisms

Definition (Pnueli '85)

A specification formalism $(M, S, \vDash)$ is expressive if $\vdash$ is a total relation.

- *i.e.*, $1_M \rightarrowtriangle \vdash ; \dashv$
- so every model has a characteristic formula

Proposition

In any expressive specification formalism, $\sqsubseteq \leftrightarrowtriangle \sqsubseteq$.

- the model preorder reduces to an equivalence
- not always what we want!

Weakly Characteristic Formulas

Definition (recall)

$s \in S$ is characteristic for $m \in M$, denoted $m \vdash s$, if

$$\forall m' \in M : m' \vDash s \iff m' \underline{\sqsupseteq} m.$$

- let's change that one:

Definition (Aceto et al '19)

$s \in S$ is weakly characteristic for $m \in M$, denoted $m \Vdash s$, if

$$\forall m' \in M : m' \vDash s \iff m' \sqsubseteq m.$$

- $\Vdash \;\leftrightarrow\; \vDash \cap (\sqsupseteq \,/\, \dashv)$
- $\dashv\!\Vdash ; \Vdash \;\rightarrow\!\!\!\!\!\circ\; \simeq$ (partial function up-to $\simeq$)
- say that $(M, S, \vDash)$ is weakly expressive if $\Vdash$ is a total relation

Incrementality

- recall: $\mathsf{Mod} \vDash \mathsf{Spec}_1$ & $\mathsf{Spec}_1 \leq \mathsf{Spec}_2 \implies \mathsf{Mod} \vDash \mathsf{Spec}_2$

Definition

A weak specification theory $(M, S, \leftarrowtail, \leq)$:

- $\leftarrowtail : M \nrightarrow S$, $\leq : S \nrightarrow S$
- $\leftarrowtail$ is total: $1_M \rightarrowtriangle \leftarrowtail ; \rightarrowtail$
- $\rightarrowtail ; \leftarrowtail \rightarrowtriangle \leq$

Proposition

- $(M, S, \leftarrowtail)$ is a weakly expressive specification formalism
- $\rightarrowtail ; \leftarrowtail \rightarrowtriangle \leq \cap \geq$: on (images of) models, modal refinement is an equivalence
- $\leftarrowtail \rightarrowtriangle \Vdash$: every model is its own characteristic formula
- $\leq \rightarrowtriangle \preceq$: modal refinement implies thorough refinement

Specification Theories

Definition (recall)

A weak specification theory $(M, S, \leftarrowtail, \leq)$:

- $\leftarrowtail : M \multimap S$, $\leq : S \multimap S$
- $\leftarrowtail$ is total: $1_M \rightarrowtriangle \leftarrowtail ; \rightarrowtail$
- $\rightarrowtail ; \leftarrowtail \rightarrowtriangle \leq$

- incrementality ✓
- the rest, not for now
- our interest now: quantities

Let's go meta

A *weak division allegory* (WDA for short) is a structure

$$\mathcal{A} = \langle |\mathcal{A}|, \mathcal{A}(), \rightarrowtriangle, 1, ^\circ, ;, \cap, \backslash \rangle,$$

where:

- $|\mathcal{A}|$ is a collection of *objects*;
- for objects $A, B \in |\mathcal{A}|$, $\mathcal{A}(A, B)$ is a collection of *arrows* with a preorder $\rightarrowtriangle$

$$\frac{x \rightarrowtriangle y \qquad x \rightarrowtriangle z}{x \rightarrowtriangle y \cap z} \qquad x \cap y \rightarrowtriangle x \qquad x \cap y \rightarrowtriangle y$$

$$\frac{x \rightarrowtriangle x' \qquad y \rightarrowtriangle y'}{x ; y \rightarrowtriangle x' ; y'} \qquad \frac{x \rightarrowtriangle x'}{x^\circ \rightarrowtriangle x'^\circ} \qquad x ; (y ; z) \leftrightarrowtriangle (x ; y) ; z \qquad 1 ; x \leftrightarrowtriangle x ; 1 \leftrightarrowtriangle x$$

$$(x ; y)^\circ \leftrightarrowtriangle y^\circ ; x^\circ \qquad 1^\circ \leftrightarrowtriangle 1 \qquad x^{\circ\circ} \leftrightarrowtriangle x \qquad x ; y \rightarrowtriangle z \Leftrightarrow y \rightarrowtriangle x \setminus z.$$

Candidates WDA

Relations $\equiv \mathcal{P}(A \times B) \equiv (A \times B) \to 2 \equiv A \to 2^B$

Candidates WDA

Relations $\equiv \mathcal{P}(A \times B) \equiv (A \times B) \to 2 \equiv A \to 2^B$
What if we replace 2^B by another set of functions?

Quantitative Specification Theories?

Definition (recall)

A weak specification theory $(M, S, \leftarrowtail, \leq)$:

$\leftarrowtail : M \nrightarrow S$, $\leq : S \nrightarrow S$

$\leftarrowtail$ is total: $\mathrm{id}_M \rightarrowtriangle \leftarrowtail ; \rightarrowtail$

$\rightarrowtail ; \leftarrowtail \rightarrowtriangle \leq$

- $\leftarrowtail$ should be quantitative: $\leftarrowtail : M \times S \to [0,1]$ (or $[0,\infty]$ if you wish)
  - (0 means "is a model"; 1, "is totally not a model"; in between, "ok kind of")
  - (it's a distance! (hemimetric))
- "$\rightarrowtriangle$" translates to "$\geq_{\mathbb{R}}$" (!), and $\mathrm{id}_M(m,n) =$ (if $m = n$ then 0 else 1)
- so by (3), $\leq$ must be quantitative, too: $\leq : S \times S \to [0,1]$
- composition of relations is infimum: $(R ; S)(x,z) = \inf_y \{R(x,y) \cdot S(y,z)\}$
- so (2) reads $\forall m : \inf\{\leftarrowtail(m,s) \mid s \in S\} = 0$: makes sense!

And Then?

Definition (proposal)

A quantitative specification theory $(M, S, \leftarrowtail, \leq)$:

$\leftarrowtail : M \times S \to [0,1]$, $\leq : S \times S \to [0,1]$

$\mathsf{id}_M \geq_{\mathbb{R}} \leftarrowtail ; \rightarrowtail$

$\rightarrowtail ; \leftarrowtail \geq_{\mathbb{R}} \leq$

- by (2): $\forall m \in M : \forall \epsilon > 0 : \exists s \in S : \leftarrowtail(m,s) < \epsilon$
- (3) implies again $\rightarrowtail ; \leftarrowtail \geq_{\mathbb{R}} \leq \cap \geq$ (and $\cap$ is max (!))
  - so $\forall s, s' : \inf\{m \in M \mid \leftarrowtail(m,s) \cdot \leftarrowtail(m,s')\} \geq \max(\leq(s,s'), \leq(s',s))$
  - (what does that mean?)
- and what about modal vs thorough refinement, approximate sets of implementations, etc.?

Conclusion?

- Specification theories can help with compositional verification
  - quantitative generalization(s): not clear
- The relational setting provides a nice framework to think about such things
  - also category theory, of course
- But it seems that the theory of quantitative ("fuzzy") relations is less well-suited than we thought
  - lots of basic stuff to develop