Specification Theories, Reloaded Relationally

Uli Fahrenberg Paul Brunet

LMF, Université Paris-Saclay

LACL, Université Paris-Est Créteil

JN GT MTV2, December 2025

LMF Laboratoire Méthodes Formelles

Motivation

models		specifications
Mod	$\models$	Spec
	model checking	

Not so easy. . .

Motivation

models specifications

$$\text{Mod} \models \text{Spec}$$

model checking

Not so easy. . .

Incremental certification / Compositional verification

- bottom-up and top-down

Wish list:

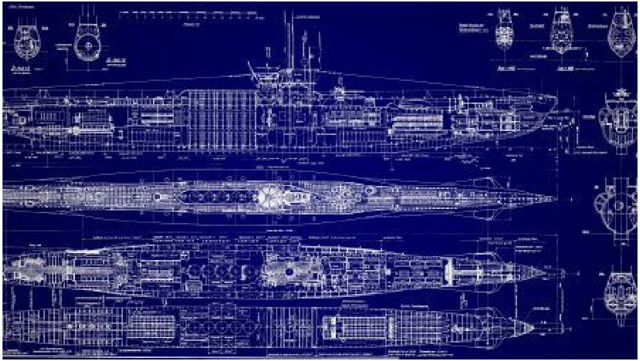
- $\text{Mod} \models \text{Spec}_1 \;\&\; \text{Spec}_1 \leq \text{Spec}_2 \implies \text{Mod} \models \text{Spec}_2$
- $\text{Mod} \models \text{Spec}_1 \;\&\; \text{Mod} \models \text{Spec}_2 \implies \text{Mod} \models \text{Spec}_1 \wedge \text{Spec}_2$
- $\text{Mod}_1 \models \text{Spec}_1 \;\&\; \text{Mod}_2 \models \text{Spec}_2 \implies \text{Mod}_1 \,\|\, \text{Mod}_2 \models \text{Spec}_1 \,\|\, \text{Spec}_2$
- $\text{Mod}_1 \models \text{Spec}_1 \;\&\; \text{Mod}_2 \models \text{Spec} / \text{Spec}_1 \implies \text{Mod}_1 \,\|\, \text{Mod}_2 \models \text{Spec}$

Compositional Verification

- $\mathrm{Mod} \models \mathrm{Spec}_1$ & $\mathrm{Spec}_1 \le \mathrm{Spec}_2 \implies \mathrm{Mod} \models \mathrm{Spec}_2$
  - incrementality
- $\mathrm{Mod} \models \mathrm{Spec}_1$ & $\mathrm{Mod} \models \mathrm{Spec}_2 \implies \mathrm{Mod} \models \mathrm{Spec}_1 \land \mathrm{Spec}_2$
  - conjunction
- $\mathrm{Mod}_1 \models \mathrm{Spec}_1$ & $\mathrm{Mod}_2 \models \mathrm{Spec}_2 \implies \mathrm{Mod}_1 \| \mathrm{Mod}_2 \models \mathrm{Spec}_1 \| \mathrm{Spec}_2$
  - compositionality
- $\mathrm{Mod}_1 \models \mathrm{Spec}_1$ & $\mathrm{Mod}_2 \models \mathrm{Spec} / \mathrm{Spec}_1 \implies \mathrm{Mod}_1 \| \mathrm{Mod}_2 \models \mathrm{Spec}$
  - 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
- Ongoing work with Paul Brunet

Specification Formalisms

Definition

A specification formalism is a structure $(M, S, \models)$ with a satisfaction relation $\models : M \mathrel{-\!\!\!\ominus\!\!\!\rightarrow} S$ between a set M of models and a set S of specifications / formulas.

- Induces preorders and equivalences:

$$\sqsubseteq \; := \; \models / \models \qquad\qquad \preceq \; := \; \models \backslash \models$$

$$\sqsubseteq\!\!\!\sqsupseteq \; := \; \sqsubseteq \cap \sqsupseteq \qquad\qquad \simeq \; := \; \preceq \cap \succeq$$

Lemma

For $m_1, m_2 \in M$, $m_1 \sqsubseteq m_2$ iff $m_2 \models s \Longrightarrow m_1 \models s$ for all $s \in S$.

Lemma

For $s_1, s_2 \in S$, $s_1 \preceq s_2$ iff $m \models s_1 \Longrightarrow m \models s_2$ for all $m \in M$.

- $\sqsubseteq\!\!\!\sqsupseteq$ 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

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

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

Expressive Specification Formalisms

Definition (Pnueli '85)

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

- *i.e.*, $\mathrm{id}_M \rightharpoonup \vdash ; \dashv$
- so every model has a characteristic formula

Proposition

In any expressive specification formalism, $\sqsubseteq \;\Leftrightarrow\; \sqsubseteq$.

- 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

$$\forall m' \in M : m' \models s \iff m' \,\underline{\square}\, m.$$

- 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

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

- $\Vdash \;\leftrightarrow\; \models \cap \left(\sqsupseteq / \mathrel{=\!|}\right)$
- $\mathrel{\dashv\!|} ; \Vdash \;\rightharpoonup\; \simeq$ (partial function up-to $\simeq$)
- say that $(M, S, \models)$ is weakly expressive if $\Vdash$ is a total relation

Incrementality

- recall: $\text{Mod} \models \text{Spec}_1 \ \& \ \text{Spec}_1 \leq \text{Spec}_2 \implies \text{Mod} \models \text{Spec}_2$

Definition

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

- $\leftarrow : M \to S$, $\leq : S \to S$
- $\leftarrow$ is total: $\text{id}_M \to \leftarrow ; \rightarrow$
- $\rightarrow ; \leftarrow \ \to \ \leq$

Proposition

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

Specification Theories

Definition (recall)

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

- $\multimapinv : M \mathrel{-\!\!\ominus\!\!\rightarrow} S$, $\leq : S \mathrel{-\!\!\ominus\!\!\rightarrow} S$
- $\multimapinv$ is total: $\mathrm{id}_M \mathrel{-\!\!\triangleright} \multimapinv \,;\, \multimap$
- $\multimap \,;\, \multimapinv \mathrel{-\!\!\triangleright} \leq$

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

Quantitative Specification Theories?

Definition (recall)

A weak specification theory $(M, S, \leftarrow, \le)$:

1. $\leftarrow : M \rightarrow S$, $\le : S \rightarrow S$
2. $\leftarrow$ is total: $\mathrm{id}_M \rightharpoonup \leftarrow ; \rightarrow$
3. $\rightarrow ; \leftarrow \rightharpoonup \le$

- $\leftarrow$ should be quantitative: $\leftarrow : M \times S \to [0,1]$ (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))
- " $\rightharpoonup$ " translates to " $\ge_\mathbb{R}$ " (!), and $\mathrm{id}_M(m,n) = (\text{if } m = n \text{ then } 0 \text{ else } 1)$
- so by (3), $\le$ must be quantitative, too: $\le : S \times S \to [0,1]$
- composition of relations is infimum: $(R ; S)(x,z) = \inf_y \{R(x,y) \cdot S(y,z)\}$
- so (2) reads $\forall m : \inf\{\leftarrow(m,s) \mid s \in S\} = 0$: makes sense!

And Then?

Definition (proposal)

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

1. $\leftarrow : M \times S \to [0,1]$, $\leq : S \times S \to [0,1]$
2. $\mathrm{id}_M \geq_{\mathbb{R}} \leftarrow ; \rightarrow$
3. $\rightarrow ; \leftarrow \geq_{\mathbb{R}} \leq$

- by (2): $\forall m \in M : \forall \epsilon > 0 : \exists s \in S : \leftarrow(m, s) < \epsilon$
- (3) implies again $\rightarrow ; \leftarrow \geq_{\mathbb{R}} \leq \cap \geq$ (and $\cap$ is max (!))
  - so $\forall s, s' : \inf\{m \in M \mid \leftarrow(m, s) \cdot \leftarrow(m, s')\} \geq \max(\leq(s, s'), \leq(s', s))$
  - (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
- Paul Brunet has convinced me that 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