Behavioral Specification Theories

Uli Fahrenberg Axel Legay

EPITA Research and Development Laboratory (LRDE), France

Université Catholique de Louvain, Belgium

ISoLA X-by-C 2020/21

Motivation

$$\underset{\text{models}}{\text{Mod}} \quad \models \quad \underset{\text{specifications}}{\text{Spec}}$$

model checking

Not so easy...

Motivation

$$\underset{\text{models}}{\text{Mod}} \quad \models \quad \underset{\text{specifications}}{\text{Spec}}$$

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

- $\text{Mod} \models \text{Spec}_1$ & $\text{Spec}_1 \leq \text{Spec}_2 \implies \text{Mod} \models \text{Spec}_2$
  - incrementality
- $\text{Mod} \models \text{Spec}_1$ & $\text{Mod} \models \text{Spec}_2 \implies \text{Mod} \models \text{Spec}_1 \wedge \text{Spec}_2$
  - conjunction
- $\text{Mod}_1 \models \text{Spec}_1$ & $\text{Mod}_2 \models \text{Spec}_2 \implies \text{Mod}_1 \| \text{Mod}_2 \models \text{Spec}_1 \| \text{Spec}_2$
  - compositionality
- $\text{Mod}_1 \models \text{Spec}_1$ & $\text{Mod}_2 \models \text{Spec} / \text{Spec}_1 \implies \text{Mod}_1 \| \text{Mod}_2 \models \text{Spec}$
  - quotient

Not so easy – but easier than model checking?

Acceptance Automata

Let Σ be a finite alphabet.

Definition

A (nondeterministic) acceptance automaton (AA) is a structure $\mathcal{A} = (S, S^0, \mathrm{Tran})$, with $S \supseteq S^0$ finite sets of states and initial states and $\mathrm{Tran} : S \to 2^{2^{\Sigma \times S}}$ an assignment of *transition constraints*.

- standard labeled transition system (LTS): $\mathrm{Tran} : S \to 2^{\Sigma \times S}$ (coalgebraic view)
- (for AA:) $\mathrm{Tran}(s) = \{M_1, M_2, \dots\}$: provide M_1 or M_2 or ...
- a disjunctive choice of conjunctive constraints
- J.-B. Raclet 2008 (but deterministic)
- note multiple initial states

Refinement

Definition

Let $\mathcal{A}_1 = (S_1, S_1^0, \text{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \text{Tran}_2)$ be AA.
A relation $R \subseteq S_1 \times S_2$ is a modal refinement if:

1. $\forall s_1^0 \in S_1^0 : \exists s_2^0 \in S_2^0 : (s_1^0, s_2^0) \in R$ (init)
2. $\forall (s_1, s_2) \in R : \forall M_1 \in \text{Tran}_1(s_1) : \exists M_2 \in \text{Tran}_2(s_2) :$ (tran)
   1. $\forall (a, t_1) \in M_1 : \exists (a, t_2) \in M_2 : (t_1, t_2) \in R$
   2. $\forall (a, t_2) \in M_2 : \exists (a, t_1) \in M_1 : (t_1, t_2) \in R$

Write $\mathcal{A}_1 \leq \mathcal{A}_2$ if there exists such a modal refinement.

- for any constraint choice M_1 there is a bisimilar choice M_2
- $\mathcal{A}_1$ has fewer choices than $\mathcal{A}_2$
- no more choices $\hat{=}$ only one $M \in \text{Tran}(s)$ $\hat{=}$ LTS
- formally: an embedding $\chi : \text{LTS} \hookrightarrow \text{AA}$
  such that $\chi(\mathcal{L}_1) \leq \chi(\mathcal{L}_2)$ iff $\mathcal{L}_1$ and $\mathcal{L}_2$ are bisimilar

A Step Back

Let Mod be a set of models with an equivalence $\sim$.

Definition

A (behavioral) specification theory for $(\text{Mod}, \sim)$ consists of

- a set Spec,
- a preorder $\leq \subseteq \text{Spec} \times \text{Spec}$, and
- a mapping $\chi : \text{Mod} \to \text{Spec}$,

such that $\forall \mathcal{M}_1, \mathcal{M}_2 \in \text{Mod} : \mathcal{M}_1 \sim \mathcal{M}_2 \iff \chi(\mathcal{M}_1) \leq \chi(\mathcal{M}_2)$.

- write $\mathcal{M} \models \mathcal{S}$ for $\chi(\mathcal{M}) \leq \mathcal{S}$
- $\chi(\mathcal{M})$: characteristic formula for $\mathcal{M}$: $\mathcal{M}' \models \chi(\mathcal{M}) \iff \mathcal{M}' \sim \mathcal{M}$
- incrementality: $\mathcal{M} \models \mathcal{S}_1 \,\&\, \mathcal{S}_1 \leq \mathcal{S}_2 \implies \mathcal{M} \models \mathcal{S}_2$
- acceptance automata $\hat{=}$ disjunctive modal transition systems $\hat{=}$ Hennessy-Milner logic with maximal fixed points
- safety properties

Logical Operations

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathsf{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \mathsf{Tran}_2)$ be AA.

Disjunction: $\mathcal{A}_1 \vee \mathcal{A}_2 = (S_1 \overset{+}{\cup} S_2, S_1^0 \overset{+}{\cup} S_2^0, \mathsf{Tran}_1 \overset{+}{\cup} \mathsf{Tran}_2)$

Conjunction: define $\pi_i : 2^{\Sigma \times S_1 \times S_2} \to 2^{\Sigma \times S_i}$ by

$$\pi_1(M) = \{(a, s_1) \mid \exists s_2 \in S_2 : (a, s_1, s_2) \in M\}$$
$$\pi_2(M) = \{(a, s_2) \mid \exists s_1 \in S_1 : (a, s_1, s_2) \in M\}$$

Let $\mathcal{A}_1 \wedge \mathcal{A}_2 = (S_1 \times S_2, S_1^0 \times S_2^0, \mathsf{Tran})$ with

$$\mathsf{Tran}((s_1, s_2)) = \{M \subseteq \Sigma \times S_1 \times S_2 \mid \pi_1(M) \in \mathsf{Tran}_1(s_1), \pi_2(M) \in \mathsf{Tran}_2(s_2)\}$$

Theorem (for all LTS $\mathcal{L}$ and AA $\mathcal{A}_1, \mathcal{A}_2$)

$$\mathcal{L} \models \mathcal{A}_1 \vee \mathcal{A}_2 \iff \mathcal{L} \models \mathcal{A}_1 \text{ or } \mathcal{L} \models \mathcal{A}_2$$
$$\mathcal{L} \models \mathcal{A}_1 \wedge \mathcal{A}_2 \iff \mathcal{L} \models \mathcal{A}_1 \ \& \ \mathcal{L} \models \mathcal{A}_2$$

Another Step Back

Let Mod be a set of models with an equivalence $\sim$.

Definition

A specification theory $(\text{Spec}, \leq, \chi)$ for $(\text{Mod}, \sim)$ is logical if $(\text{Spec}, \leq)$ forms a bounded distributive lattice up to $\leq \cap \geq$.

$\Rightarrow$ have least upper bound $\vee$ and greatest lower bound $\wedge$

$\Rightarrow$ bottom specification **ff** $(\forall \mathcal{M} \in \text{Mod} : \mathcal{M} \not\models \mathbf{ff})$

$\Rightarrow$ top specification **tt** $(\forall \mathcal{M} \in \text{Mod} : \mathcal{M} \models \mathbf{tt})$

$\Rightarrow$ double distributivity

- everything up to modal equivalence $\equiv = \leq \cap \geq$
- holds for acceptance automata, disjunctive modal transition systems, and Hennessy-Milner logic with maximal fixed points

Structural Operations: Composition

Let $\mathcal{A}_1 = (S_1, S_1^0, \text{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \text{Tran}_2)$ be AA.

For $M_1 \subseteq \Sigma \times S_1$ and $M_2 \subseteq \Sigma \times S_2$, define

$$M_1 \| M_2 = \{(a, (t_1, t_2)) \mid (a, t_1) \in M_1, (a, t_2) \in M_2\}$$

(assumes CSP synchronization, but can be generalized)

Let $\mathcal{A}_1 \| \mathcal{A}_2 = (S_1 \times S_2, S_1^0 \times S_2^0, \text{Tran})$ with

$$\text{Tran}((s_1, s_2)) = \{M_1 \| M_2 \mid M_1 \in \text{Tran}_1(s_1), M_2 \in \text{Tran}_2(s_2)\}$$

Theorem (independent implementability)

For all AA $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$, $\mathcal{A}_4$:

$$\mathcal{A}_1 \leq \mathcal{A}_3 \;\&\; \mathcal{A}_2 \leq \mathcal{A}_4 \implies \mathcal{A}_1 \| \mathcal{A}_2 \leq \mathcal{A}_3 \| \mathcal{A}_4$$

Structural Operations: Quotient

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$ be AA.

Define $\mathcal{A}_1 / \mathcal{A}_2 = (S, S^0, \mathrm{Tran})$:

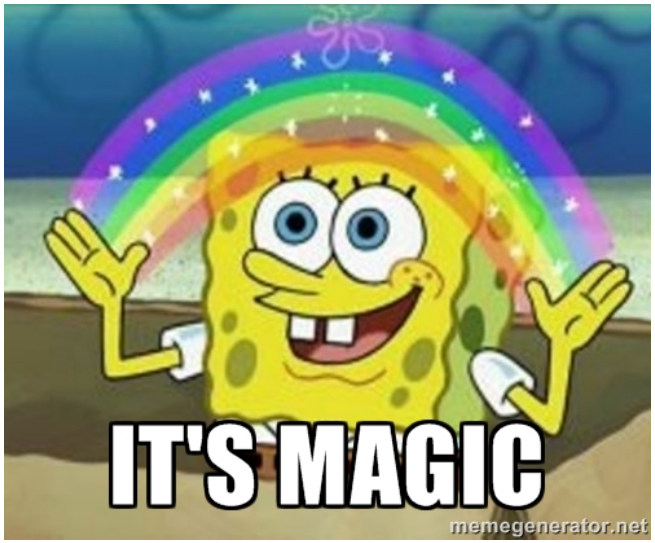
- $S = 2^{S_1 \times S_2}$
- write $S_2^0 = \{s_2^{0,1}, \ldots, s_2^{0,p}\}$ and let $S^0 = \{\{(s_1^{0,q}, s_2^{0,q}) \mid q \in \{1, \ldots, p\}\} \mid \forall q : s_1^{0,q} \in S_1^0\}$
- $\mathrm{Tran} =$

Structural Operations: Quotient

Let $\mathcal{A}_1 = (S_1, S_1^0, \text{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \text{Tran}_2)$ be AA.

Define $\mathcal{A}_1 / \mathcal{A}_2 = (S, S^0, \text{Tran})$:

- $S = 2^{S_1 \times S_2}$
- write $S_2^0 = \{s_2^{0,1}, \ldots, s_2^{0,p}\}$ and let $S^0 = \{\{(s_1^{0,q}, s_2^{0,q}) \mid q \in \{1, \ldots, p\}\} \mid \forall q : s_1^{0,q} \in S_1^0\}$
- Tran =



Structural Operations: Quotient

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$ be AA.

Define $\mathcal{A}_1/\mathcal{A}_2 = (S, S^0, \mathrm{Tran})$:

- $S = 2^{S_1 \times S_2}$
- write $S_2^0 = \{s_2^{0,1}, \ldots, s_2^{0,p}\}$ and let $S^0 = \{\{(s_1^{0,q}, s_2^{0,q}) \mid q \in \{1, \ldots, p\}\} \mid \forall q : s_1^{0,q} \in S_1^0\}$
- $\mathrm{Tran} = \ldots$

Theorem

For all AA $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$:

$$\mathcal{A}_1 \| \mathcal{A}_2 \leq \mathcal{A}_3 \iff \mathcal{A}_2 \leq \mathcal{A}_3 / \mathcal{A}_1$$

- up to $\equiv$, $/$ is the adjoint (or residual) of $\|$

A Step Back, Again

Let Mod be a set of models with an equivalence $\sim$.

Definition

A complete specification theory for $(\text{Mod}, \sim)$ is $(\text{Spec}, \leq, \|, \chi)$ such that $(\text{Spec}, \leq, \chi)$ is a specification theory for $(\text{Mod}, \sim)$ and $(\text{Spec}, \leq, \|)$ forms a bounded distribute commutative residuated lattice up to $\equiv$.

$\Rightarrow$ $\|$ distributes over $\vee$ and has a unit U, up to $\equiv$

$\Rightarrow$ $\|$ has a residual $/$, up to $\equiv$

- a compositional algebra of specifications: for example,

$$(\mathcal{S}_1 \wedge \mathcal{S}_2)/\mathcal{S}_3 \equiv \mathcal{S}_1/\mathcal{S}_3 \wedge \mathcal{S}_2/\mathcal{S}_3$$

$$\mathcal{S}_1 \| (\mathcal{S}_2/\mathcal{S}_1) \leq \mathcal{S}_2 \qquad (\mathcal{S}_1 \| \mathcal{S}_2)/\mathcal{S}_1 \leq \mathcal{S}_2$$

$$\bot \| \mathcal{S} \equiv \bot \qquad \mathcal{S}/\mathrm{U} \equiv \mathcal{S} \qquad \mathrm{U} \leq \mathcal{S}/\mathcal{S} \qquad \mathrm{U} \equiv \bot/\bot$$

$$(\mathcal{S}_1/\mathcal{S}_2)/\mathcal{S}_3 \equiv \mathcal{S}_1/(\mathcal{S}_2 \| \mathcal{S}_3)$$

$$(\mathrm{U}/\mathcal{S}_1) \| (\mathrm{U}/\mathcal{S}_2) \leq \mathrm{U}/(\mathcal{S}_1 \| \mathcal{S}_2)$$

A Step Back, Again

Let Mod be a set of models with an equivalence $\sim$.

Definition

A complete specification theory for $(\text{Mod}, \sim)$ is $(\text{Spec}, \leq, \|, \chi)$ such that $(\text{Spec}, \leq, \chi)$ is a specification theory for $(\text{Mod}, \sim)$ and $(\text{Spec}, \leq, \|)$ forms a bounded distribute commutative residuated lattice up to $\equiv$.

$\Rightarrow$ $\|$ distributes over $\vee$ and has a unit U, up to $\equiv$

$\Rightarrow$ $\|$ has a residual $/$, up to $\equiv$

- a compositional algebra of specifications
- relation to linear logic and Girard quantales

Some Extensions

Specifications	Models	L	C	Q	Notes
HML^R, DMTS, AA	LTS, bisim.	✓	✓	✓	bisimulation
HML^R, DMTS, AA	LTS, any	✗	✗	✗	any equivalence in LTBT spectrum
DMTS	LTS, fail./div.	≈	✓	✗	failure/divergence equivalence; no disjunction
MECS	ECA, t.bisim.	≈	✓	✓	timed bisim.; no disjunction
TIOA	TIOA, t.bisim.	≈	✓	≈	no disjunction; weak quotient
IMC	PA, p.bisim.	✗	✗	✗	probabilistic bisim.
APA	PA, p.bisim.	≈	✓	✗	no disjunction

(Logical; Compositional; Qomplete)

Conclusion?

- incrementality: $\mathcal{M} \models \mathcal{S}_1 \,\&\, \mathcal{S}_1 \leq \mathcal{S}_2 \implies \mathcal{M} \models \mathcal{S}_2$
- conjunction: $\mathcal{M} \models \mathcal{S}_1 \,\&\, \mathcal{M} \models \mathcal{S}_2 \iff \mathcal{M} \models \mathcal{S}_1 \wedge \mathcal{S}_2$
- disjunction: $\mathcal{M} \models \mathcal{S}_1$ or $\mathcal{M} \models \mathcal{S}_2 \iff \mathcal{M} \models \mathcal{S}_1 \vee \mathcal{S}_2$
- compositionality: $\mathcal{M}_1 \models \mathcal{S}_1 \,\&\, \mathcal{M}_2 \models \mathcal{S}_2 \implies \mathcal{M}_1 \| \mathcal{M}_2 \models \mathcal{S}_1 \| \mathcal{S}_2$
- quotient: $\mathcal{M}_1 \models \mathcal{S}_1 \,\&\, \mathcal{M}_2 \models \mathcal{S} / \mathcal{S}_1 \implies \mathcal{M}_1 \| \mathcal{M}_2 \models \mathcal{S}$
- safety properties

- Are these all the properties we want?
- What about real time, probabilities, hybrid systems?

- Adding concatenation into the mix $\rightsquigarrow$ some type of residuated concurrent Kleene algebra: further work
- Robust specification theories, with refinement replaced by distance: OK; but what is the algebra?