# Behavioral Specification Theories

Uli Fahrenberg

École polytechnique, Palaiseau, France

Sheffield June 27, 2019

# Motivation

models specifications

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

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

- $\text{Mod} \models \text{Spec}_1 \;\&\; \text{Spec}_1 \leq \text{Spec}_2 \implies \text{Mod} \models \text{Spec}_2$
  - 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?

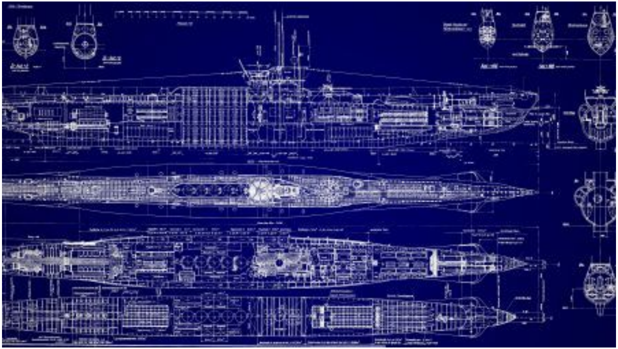
# Compositional Verification

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

Not so easy – but easier than model checking?

“Holy Grail”?

# 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??

# Acceptance Automata

Let $\Sigma$ be a finite alphabet.

**Definition**

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

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

# Acknowledgement


- This is joint work with Nikola Beneš, Benoît Delahaye, Jan Křetínský, Axel Legay, and Louis-Marie Traonouez
- based on papers at CONCUR 2013, FACS 2014, ICTAC 2014, and SOFSEM 2017
- subsequently in Soft Computing 22(4):2018, Information & Computation (to appear), and Logical Methods in CS (submitted)

# Refinement

## Definition

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.
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. $\forall (s_1, s_2) \in R : \forall M_1 \in \mathrm{Tran}_1(s_1) : \exists M_2 \in \mathrm{Tran}_2(s_2) :$ (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 $\triangleq$ only one $M \in \mathrm{Tran}(s)$ $\triangleq$ LTS
- formally: an embedding $\chi : \mathrm{LTS} \hookrightarrow \mathrm{AA}$
  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 $(\mathsf{Mod}, \sim)$ consists of

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

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

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

# Logical Operations

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

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

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

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

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

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

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

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

# Another Step Back

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

**Definition (ad hoc)**

A specification theory $(\mathsf{Spec}, \leq, \chi)$ for $(\mathsf{Mod}, \sim)$ is nice if $(\mathsf{Spec}, \leq)$ 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** $(\forall \mathcal{M} \in \mathsf{Mod} : \mathcal{M} \not\models \mathbf{ff})$
- $\Rightarrow$ top specification **tt** $(\forall \mathcal{M} \in \mathsf{Mod} : \mathcal{M} \models \mathbf{tt})$
- $\Rightarrow$ 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 $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$ 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 $\mathcal{A}_1 \| \mathcal{A}_2 = (S_1 \times S_2, S_1^0 \times S_2^0, \mathrm{Tran})$ with

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

**Theorem (independent implementability)**

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

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

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

# Structural Operations: Quotient

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$ 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 $S_2^0 = \{s_2^{0,1}, \dots, s_2^{0,p}\}$ and let
  $S^0 = \{\{(s_1^{0,q}, s_2^{0,q}) \mid q \in \{1, \dots, p\}\} \mid \forall q : s_1^{0,q} \in S_1^0\}$
- $\mathrm{Tran} =$ 

# Structural Operations: Quotient

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$ 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 $S_2^0 = \{s_2^{0,1}, \dots, s_2^{0,p}\}$ and let $S^0 = \{\{(s_1^{0,q}, s_2^{0,q}) \mid q \in \{1, \dots, p\}\} \mid \forall q : s_1^{0,q} \in S_1^0\}$
- $\mathrm{Tran} = \quad \dots$

**Theorem**

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

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

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

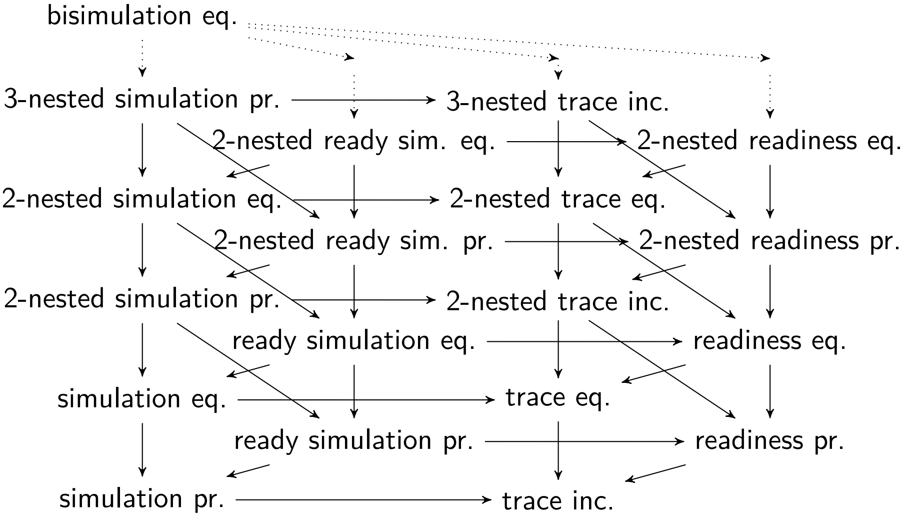
- $\Rightarrow$ $\|$ distributes over $\vee$ and has a unit $\mathrm{U}$, up to $\equiv$
- $\Rightarrow$ $\|$ has a residual $/$, up to $\equiv$
- a compositional algebra of specifications
- relation to linear logic and Girard quantales

1. Motivation
2. Acceptance Automata
3. Specification Theories for Real Time, Probabilities, etc.
4. Conclusion

# Specification Theories for LTS

- (disjunctive) modal transition systems: [Larsen-Xinxin 1989-90]
- equivalence with acceptance automata and Hennessy-Milner logic with greatest fixed points: [Larsen-Boudol 1992], [Beneš-Delahaye-UF *et al.* 2013]
- modal transition systems with data: [Bauer-Juhl-Larsen *et al.* 2012]
- parametric modal transition systems: [Beneš-Křetínský-Larsen *et al.* 2011]
- for deadlock equivalence: [Bujtor-Sorokin-Vogler 2015]

# [UF-Legay SOFSEM 2017]: The Linear-Time–Branching-Time Spectrum of Specification Theories

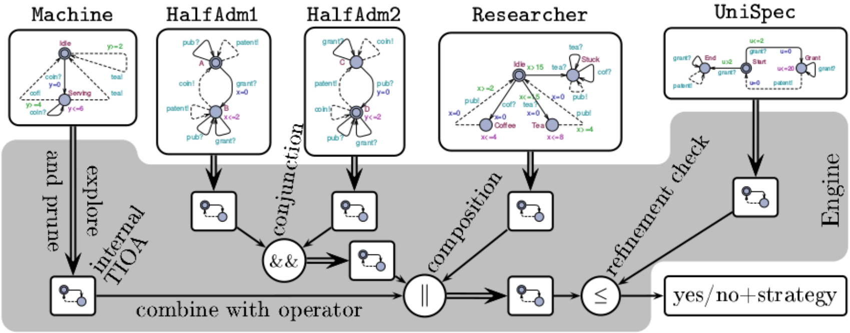


# Specification Theories for Real-Time Systems

Timed input-output automata:

- [David-Larsen-Legay *et al.*: Real-time specifications, STTT 2015], [David-Larsen-Legay *et al.*: Compositional verification of real-time systems using ECDAR, STTT 2012]
- complete, with quotient, but without disjunction
- only for deterministic specifications
- tool support: ECDAR / UPPAAL TiGa (Aalborg)
- some work on robustness and implementability: [Larsen-Legay-Traonouez *et al.*: Robust synthesis for real-time systems, TCS 2014]

# Timed Input-Output Automata



# Specification Theories for Real-Time Systems, contd.

Modal event-clock specifications:

- [Bertrand-Legay-Pinchinat *et al.*: Modal event-clock specifications for timed component-based design, SCP 2012]
- complete, with quotient, but without disjunction
- only for deterministic specifications
- some work on robustness: [UF-Legay 2012]

Synchronous time-triggered interface theories:

- [Delahaye-UF-Henzinger *et al.* 2012]
- no quotient, no real conjunction, no implementation
- relation to BIP (Grenoble)

# Specification Theories for Probabilistic (Timed) Systems

Abstract probabilistic automata:

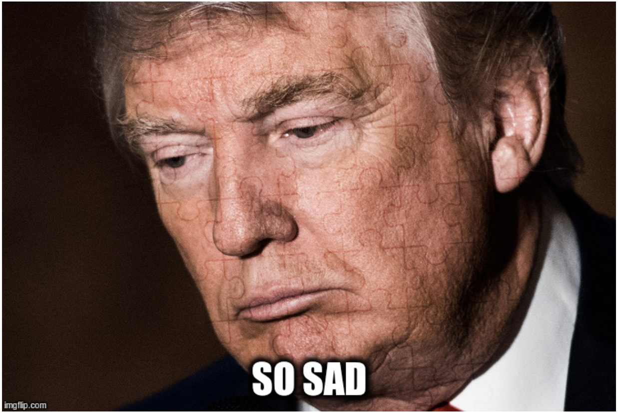
- [Delahaye-Katoen-Larsen *et al.*: Abstract probabilistic automata, I&C 2013], [Delahaye-UF-Larsen *et al.* 2014]
- no quotient, no disjunction, toy implementation

Abstract probabilistic event-clock automata:

- [Han-Krause-Kwiatkowska *et al.* 2013]
- no quotient, no disjunction, no implementation, other problems

# Specification Theories for Hybrid Systems

# Specification Theories for Hybrid Systems



# Interfaces and Contracts

Modal interface automata

- [Lüttgen-Vogler: Modal interface automata, LMCS 2013]
- interface automata: [de Alfaro-Henzinger 2001]
- inputs vs outputs
- complete, without quotient

From specifications to contracts:

- [Bauer-David-Hennicker *et al.* 2012]
- complete specification theory $\Longrightarrow$ contract theory
- in a timed setting: [Le-Passerone-UF *et al.*: A tag contract framework for modeling heterogeneous systems, SCP 2016]

# Robust Specification Theories

**Definition (recall)**

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

- for robustness: replace $\sim$ by pseudometric $d_{\mathsf{Mod}}$
- (such that $d_{\mathsf{Mod}}(\mathcal{M}_1, \mathcal{M}_2) = 0$ iff $\mathcal{M}_1 \sim \mathcal{M}_2$)
- replace $\leq$ by non-symmetric pseudometric $d$ ("hemimetric")
- ($d_{\mathsf{Mod}}$ and $d$ are related via $\chi$)
- instead of $\mathcal{M} \models \mathcal{S}_1 \;\&\; \mathcal{S}_1 \leq \mathcal{S}_2 \implies \mathcal{M} \models \mathcal{S}_2$,
  want $\quad d(\mathcal{M}, \mathcal{S}_1) + d(\mathcal{S}_1, \mathcal{S}_2) \geq d(\mathcal{M}, \mathcal{S}_2)$
- $d(\mathcal{S}, \mathcal{S}_1 \wedge \mathcal{S}_2) = \max(d(\mathcal{S}, \mathcal{S}_1), d(\mathcal{S}, \mathcal{S}_2), \infty)$
- $d(\mathcal{S}_1 \vee \mathcal{S}_2, \mathcal{S}) = \max(d(\mathcal{S}_1, \mathcal{S}), d(\mathcal{S}_2, \mathcal{S}), \infty)$

# Robust Specification Theories, contd.

**Definition (recall)**

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 $\equiv$.

- for independent implementability, want uniform continuity for $\|$: a function $C : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ such that we can replace $\mathcal{S}_1 \leq \mathcal{S}_3 \,\&\, \mathcal{S}_2 \leq \mathcal{S}_4 \implies \mathcal{S}_1 \| \mathcal{S}_2 \leq \mathcal{S}_3 \| \mathcal{S}_4$ with $C(d(\mathcal{S}_1, \mathcal{S}_3), d(\mathcal{S}_2, \mathcal{S}_4)) \geq d(\mathcal{S}_1 \| \mathcal{S}_2, \mathcal{S}_3 \| \mathcal{S}_4)$
- for quotient, instead of $\mathcal{S}_1 \| \mathcal{S}_2 \leq \mathcal{S}_3 \iff \mathcal{S}_2 \leq \mathcal{S}_3 / \mathcal{S}_1$ want $d(\mathcal{S}_1 \| \mathcal{S}_2, \mathcal{S}_3) = d(\mathcal{S}_2, \mathcal{S}_3 / \mathcal{S}_1)$
- [UF-Legay TCS 2014], [UF-Legay Acta Inf. 2014], [UF-Křetínský-Legay *et al.* 2014]

# Conclusion?

- incrementality: $\mathcal{M} \models \mathcal{S}_1 \ \& \ \mathcal{S}_1 \le \mathcal{S}_2 \implies \mathcal{M} \models \mathcal{S}_2$
- 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?
- Also need robustness

- Long way

  from acceptance automata

  to hybrid systems

  to industry . . .