A Linear-Time–Branching-Time Spectrum of Behavioral Specification Theories

Uli Fahrenberg Axel Legay

École polytechnique, Palaiseau, France

Inria Rennes, France

SOFSEM 2017

Motivation

- Specification theories allow incremental and compositional reasoning
  - $\text{Mod} \models \text{Spec}_1 \;\&\; \text{Spec}_1 \leq \text{Spec}_2 \implies \text{Mod} \models \text{Spec}_2$
  - $\text{Mod} \models \text{Spec}_1 \;\&\; \text{Mod} \models \text{Spec}_2 \implies \text{Mod} \models \text{Spec}_1 \land \text{Spec}_2$
  - $\text{Mod}_1 \models \text{Spec}_1 \;\&\; \text{Mod}_2 \models \text{Spec}_2$
    $\implies \text{Mod}_1 \| \text{Mod}_2 \models \text{Spec}_1 \| \text{Spec}_2$
- mostly developed for bisimulation
- [Bujtor-Vogler'15] show that specification theories for other semantics are also useful

Our goal: Develop comprehensive theory of specification theories for different semantics

- here: first step

Some Old Hats: Adequacy

Let Mod be a set of models.

[Larsen'90], but much older:

- a specification formalism for Mod: (Spec, $\models$)
  - $\models \subseteq \text{Mod} \times \text{Spec}$ satisfaction
  - model checking: for $\mathcal{I} \in \text{Mod}$ and $\mathcal{S} \in \text{Spec}$, decide $\mathcal{I} \models \mathcal{S}$
- for $\mathcal{S} \in \text{Spec}$: $[\![\mathcal{S}]\!] = \{\mathcal{I} \in \text{Mod} \mid \mathcal{I} \models \mathcal{S}\}$ set of implementations
- semantic refinement on Spec: $\mathcal{S}_1 \preceq \mathcal{S}_2$ iff $[\![\mathcal{S}_1]\!] \subseteq [\![\mathcal{S}_2]\!]$
- for $\mathcal{I} \in \text{Mod}$: $\text{Th}(\mathcal{I}) = \{\mathcal{S} \in \text{Spec} \mid \mathcal{I} \models \mathcal{S}\}$ set of theories
- theory inclusion on Mod: $\mathcal{I} \sqsubseteq \mathcal{J}$ iff $\text{Th}(\mathcal{I}) \subseteq \text{Th}(\mathcal{J})$
- theory equivalence on Mod: $\sqsubseteq\!\!\!\!\sqsupseteq \; = \; \sqsubseteq \cap \sqsupseteq$

[Hennessy-Milner'85]: (Spec, $\models$) is adequate for $\sqsubseteq\!\!\!\!\sqsupseteq$

Some Old Hats: Expressiveness

[Pnueli'85]:

- $\mathcal{S} \in$ Spec is a characteristic formula for $\mathcal{I} \in$ Mod if $\mathcal{I} \models \mathcal{S}$ and $\forall \mathcal{J} \in$ Mod : $J \models \mathcal{S} \implies \mathcal{J} \sqsupseteq \mathcal{I}$
- (Spec, $\models$) is expressive if every $\mathcal{I} \in$ Mod has a characteristic formula

Lemma (new!)

If Spec is expressive, then $\sqsubseteq = \sqsupseteq$.

Proof.

- Let $\mathcal{I} \sqsubseteq \mathcal{J}$
- Let $\mathcal{S}$ be characteristic for $\mathcal{I}$, then $\mathcal{S} \in \text{Th}(\mathcal{I})$
- But $\text{Th}(\mathcal{I}) \subseteq \text{Th}(\mathcal{J})$, hence $\mathcal{S} \in \text{Th}(\mathcal{J})$
- Thus $\mathcal{J} \models \mathcal{S}$
- $\mathcal{S}$ is characteristic, hence $\mathcal{J} \sqsupseteq \mathcal{I}$

A Silly Example

Spec $= 2^{\mathsf{Mod}}$, $\models \; = \; \in$:

- $[\![\mathcal{S}]\!] = \{\mathcal{I} \mid \mathcal{I} \in \mathcal{S}\} = \mathcal{S}$
- $\mathcal{S}_1 \preceq \mathcal{S}_2$ iff $\mathcal{S}_1 \subseteq \mathcal{S}_2$
- $\mathsf{Th}(\mathcal{I}) = \{\mathcal{S} \subseteq \mathsf{Mod} \mid \mathcal{I} \in \mathcal{S}\}$
- $\mathcal{I} \sqsubseteq \mathcal{J}$ iff $\mathsf{Th}(\mathcal{I}) \subseteq \mathsf{Th}(\mathcal{J})$
  iff $\{\mathcal{S} \mid \mathcal{I} \in \mathcal{S}\} \subseteq \{\mathcal{S} \mid \mathcal{J} \in \mathcal{S}\}$ iff $\mathcal{I} = \mathcal{J}$
- hence $\sqsupseteq \; = \; \sqsubseteq \; = \; =$
- characteristic formula for $\mathcal{I}$: $\{\mathcal{I}\}$
- Hence $(2^{\mathsf{Mod}}, \in)$ is expressive and adequate for $=$

(This is not very useful.)

A Less Silly Example

Hennessy-Milner logic (without negation):

- Mod = labeled transition systems over some Σ
- Spec $\ni \phi, \psi ::= \mathbf{tt} \mid \mathbf{ff} \mid \phi \wedge \psi \mid \phi \vee \psi \mid \langle a \rangle \phi \mid [a]\phi \quad (a \in \Sigma)$
- admits complementation: $\mathbf{tt}^c = \mathbf{ff}$, $\mathbf{ff}^c = \mathbf{tt}$, $(\phi \wedge \psi)^c = \phi^c \vee \psi^c$, $(\phi \vee \psi)^c = \phi^c \wedge \psi^c$, $(\langle a \rangle \phi)^c = [a]\phi^c$, $([a]\phi)^c = \langle a \rangle \phi^c$
  - "semantic negation": for all ϕ, $[\![\phi^c]\!] = \text{Mod} \setminus [\![\phi]\!]$
- $\mathcal{I} \sqsubseteq \mathcal{J}$ iff $\forall \phi : \mathcal{I} \models \phi \implies \mathcal{J} \models \phi$ iff $\forall \phi : \mathcal{J} \models \phi^c \implies \mathcal{I} \models \phi^c$ iff $\mathcal{J} \sqsubseteq \mathcal{I}$
  - hence $\sqsupseteq \; = \; \sqsubseteq$
- adequate for bisimulation, but not expressive

Hennessy-Milner logic with (recursion and) greatest fixed points:

- expressive
- [Beneš-UF-*et al.* 13/14]: equivalent to DMTS

Specification Theories

Definition (not new; just a *clarification*)

A specification theory for Mod is a specification formalism (Spec, $\models$) for Mod, together with a mapping χ : Mod $\to$ Spec and a preorder $\leq$ on Spec, called modal refinement, subject to the following conditions:

- for every $\mathcal{I} \in$ Mod, $\chi(\mathcal{I})$ is a characteristic formula for $\mathcal{I}$;
- for all $\mathcal{I} \in$ Mod and all $\mathcal{S} \in$ Spec, $\mathcal{I} \models \mathcal{S}$ iff $\chi(\mathcal{I}) \leq \mathcal{S}$.

Lemma (also not new)

- For all $\mathcal{S}_1, \mathcal{S}_2 \in$ Spec, $\mathcal{S}_1 \leq \mathcal{S}_2$ implies $\mathcal{S}_1 \preceq \mathcal{S}_2$.
- For all $\mathcal{I}, \mathcal{J} \in$ Mod, the following are equivalent: $\chi(\mathcal{I}) \leq \chi(\mathcal{J})$, $\chi(\mathcal{I}) \geq \chi(\mathcal{J})$, $\chi(\mathcal{I}) \preceq \chi(\mathcal{J})$, $\chi(\mathcal{I}) \succeq \chi(\mathcal{J})$, $\mathcal{I} \sqsubseteq \mathcal{J}$

Specification Theories

Lemma (new?)

Let Spec be a set, $\chi : \text{Mod} \to \text{Spec}$ a mapping and $\leq \subseteq \text{Spec} \times \text{Spec}$ a preorder. If the restriction of $\leq$ to the image of χ is symmetric, then $(\text{Spec}, \chi, \leq)$ is a specification theory for Mod.

Proof.

- Let $\mathcal{I} \in \text{Mod}$ — show that $\chi(\mathcal{I})$ is characteristic for $\mathcal{I}$
- reflexivity $\implies \chi(\mathcal{I}) \leq \chi(\mathcal{I}) \implies \mathcal{I} \models \chi(\mathcal{I})$
  - $\models$ is *defined* by $\mathcal{I} \models \mathcal{S}$ iff $\chi(\mathcal{I}) \leq \mathcal{S}$
- Let $\mathcal{J} \models \chi(\mathcal{I})$ — show $\mathcal{J} \sqsupseteq \mathcal{I}$, *i.e.* $\text{Th}(\mathcal{J}) = \text{Th}(\mathcal{I})$
- $\mathcal{S} \in \text{Th}(\mathcal{I}) \Rightarrow \mathcal{I} \models \mathcal{S} \Rightarrow \chi(\mathcal{J}) \leq \chi(\mathcal{I}) \leq \mathcal{S} \Rightarrow \mathcal{J} \models \mathcal{S} \Rightarrow \mathcal{S} \in \text{Th}(\mathcal{J})$
- $\mathcal{S} \in \text{Th}(\mathcal{J}) \Rightarrow \mathcal{J} \models \mathcal{S} \Rightarrow \chi(\mathcal{I}) \leq \chi(\mathcal{J}) \leq \mathcal{S} \Rightarrow \mathcal{I} \models \mathcal{S} \Rightarrow \mathcal{S} \in \text{Th}(\mathcal{I})$

Specification Theories?

Have (qua definition):

- incrementality: $\mathcal{I} \models \mathcal{S}_1 \,\&\, \mathcal{S}_1 \le \mathcal{S}_2 \implies \mathcal{I} \models \mathcal{S}_2$

Usually also want:

- conjunction: $\mathcal{I} \models \mathcal{S}_1 \,\&\, \mathcal{I} \models \mathcal{S}_2 \iff \mathcal{I} \models \mathcal{S}_1 \wedge \mathcal{S}_2$
- compositionality: $\mathcal{I}_1 \models \mathcal{S}_1 \,\&\, \mathcal{I}_2 \models \mathcal{S}_2 \implies \mathcal{I}_1 \| \mathcal{I}_2 \models \mathcal{S}_1 \| \mathcal{S}_2$
- quotient: $\mathcal{I}_1 \models \mathcal{S}_1 \,\&\, \mathcal{I}_2 \models \mathcal{S} / \mathcal{S}_1 \implies \mathcal{I}_1 \| \mathcal{I}_2 \models \mathcal{S}$

But not in this paper.

Recall Motivation

- Specification theories allow incremental and compositional reasoning
  - $\text{Mod} \models \text{Spec}_1 \;\&\; \text{Spec}_1 \leq \text{Spec}_2 \implies \text{Mod} \models \text{Spec}_2$
- mostly developed for bisimulation
- [Bujtor-Vogler'15] show that specification theories for other semantics are also useful

Our goal: Develop comprehensive theory of specification theories for different semantics

- our paper: a linear-time–branching-time spectrum of specification theories
- here: only for ready simulation equivalence
- based on DMTS

DMTS

From now on: Mod = LTS – finite labeled transition systems (S, s^0, T)

Definition ([Larsen-Xinxin'90])

A disjunctive modal transition system (DMTS) is $\mathcal{D} = (S, S^0, \dashrightarrow, \longrightarrow)$:

- $S \supseteq S^0$ finite sets of states and initial states
- $\dashrightarrow \subseteq S \times \Sigma \times S$ may-transitions
- $\longrightarrow \subseteq S \times 2^{\Sigma \times S}$ disjunctive must-transitions

It is assumed that for all $(s, N) \in \longrightarrow$ and all $(a, t) \in N$, $(s, a, t) \in \dashrightarrow$.

Definition ([Larsen-Xinxin'90])

For an LTS $\mathcal{I} = (S, s^0, T)$, let $\chi(\mathcal{I}) = (S, \{s^0\}, \dashrightarrow, \longrightarrow)$ be the DMTS with $\dashrightarrow = T$ and $\longrightarrow = \{(s, \{(a, t)\}) \mid (s, a, t) \in T\}$.

DMTS and Bisimilarity

Definition (old)

A modal refinement of two DMTS $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1)$, $\mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2)$ is a relation $R \subseteq S_1 \times S_2$ for which it holds of all $(s_1, s_2) \in R$ that

- $\forall s_1 \overset{a}{\dashrightarrow}_1 t_1 : \exists s_2 \overset{a}{\dashrightarrow}_2 t_2 : (t_1, t_2) \in R$;
- $\forall s_2 \longrightarrow_2 N_2 : \exists s_1 \longrightarrow_1 N_1 : \forall (a, t_1) \in N_1 : \exists (a, t_2) \in N_2 : (t_1, t_2) \in R$;

and such that for all $s_1^0 \in S_1^0$, there exists $s_2^0 \in S_2^0$ for which $(s_1^0, s_2^0) \in R$.

Write $\mathcal{D}_1 \leq \mathcal{D}_2$ if there exists a modal refinement $R \subseteq S_1 \times S_2$.

Theorem (old)

$(\text{DMTS}, \chi, \leq)$ is a specification theory for LTS adequate for bisimilarity.

Ready Simulation Equivalence

[Larsen-Skou'89]

- a ready simulation of LTS $\mathcal{I}_1 = (S_1, s_1^0, T_1)$, $\mathcal{I}_2 = (S_2, s_2^0, T_2)$: a relation $R \subseteq S_1 \times S_2$ such that $(s_1^0, s_2^0) \in R$ and for all $(s_1, s_2) \in R$,
  - for all $(s_1, a, t_1) \in T_1$, there is $(s_2, a, t_2) \in T_2$ with $(t_1, t_2) \in R$;
  - for all $(s_2, a, t_2) \in T_2$, there is $(s_1, a, t_1) \in T_1$.
- $\mathcal{I}_1$ and $\mathcal{I}_2$ ready simulation equivalent if there exist a ready simulation $R_1 \subseteq S_1 \times S_2$ and a ready simulation $R_2 \subseteq S_2 \times S_1$.
  - (Compare: $\mathcal{I}_1$ and $\mathcal{I}_2$ bisimilar if there exists a (ready) simulation $R \subseteq S_1 \times S_2$ such that $R^{\text{inv}} \subseteq S_2 \times S_1$ is also a (ready) simulation.)

DMTS and Ready Simulation Equivalence

Definition

Let $\mathcal{D}_1 = (S_1, S_1^0, \dashrightarrow_1, \longrightarrow_1), \mathcal{D}_2 = (S_2, S_2^0, \dashrightarrow_2, \longrightarrow_2) \in$ DMTS.
A ready simulation refinement consists of $R_1, R_2 \subseteq S_1 \times S_2$ such that

- $\forall s_1^0 \in S_1^0 : \exists s_2^0 \in S_2^0 : (s_1^0, s_2^0) \in R_1$ and
  $\forall s_2^0 \in S_2^0 : \exists s_1^0 \in S_1^0 : (s_1^0, s_2^0) \in R_2$;
- for all $(s_1, s_2) \in R_1$:
  - $\forall s_1 \overset{a}{\dashrightarrow}_1 t_1 : \exists s_2 \overset{a}{\dashrightarrow}_2 t_2 : (t_1, t_2) \in R_1$;
  - $\forall s_2 \overset{a}{\dashrightarrow}_2 t_2 : \exists s_1 \overset{a}{\dashrightarrow}_1 t_1$;
- for all $(s_1, s_2) \in R_2$:
  - $\forall s_2 \longrightarrow_2 N_2 : \exists s_1 \longrightarrow_1 N_1 : \forall (a, t_1) \in N_1 : \exists (a, t_2) \in N_2 : (t_1, t_2) \in R_2$;
  - $\forall s_1 \longrightarrow_1 N_1 : \exists s_2 \longrightarrow_2 N_2 : \forall (a, t_2) \in N_2 : \exists (a, t_1) \in N_1$.

Theorem: DMTS with r.s.r. is a spec. theory for LTS adequate for r.s.e.

Conclusion and Further Work

- Specification theories allow incremental and compositional reasoning
- We develop specification theories for all equivalences in van Glabbeek's linear-time–branching-time spectrum
- *I.e.* for simulation equivalence, ready simulation equivalence, nested simulation equivalence, trace equivalence, possible-futures equivalence, failure equivalence, etc.

- But without conjunction and composition, usefulness debatable $\ddot\smile$
- We're working on it!

- Secret tool: generalized simulation games [UF-Legay'14]

References

- [Hennessy-Milner'85] Algebraic Laws for Nondeterminism and Concurrency (J. ACM)
- [Pnueli'85] Linear and Branching Structures in the Semantics and Logics of Reactive Systems (ICALP)
- [Larsen-Skou'89] Bisimulation Through Probabilistic Testing (POPL)
- [Larsen'90] Ideal Specification Formalism = Expressivity + Compositionality + Decidability + Testability + . . . (CONCUR)
- [Larsen-Xinxin'90] Equation Solving Using Modal Transition Systems (LICS)

References

- [Beneš-UF-*et al.* 13] Hennessy-Milner Logic with Greatest Fixed Points as a Complete Behavioural Specification Theory (CONCUR)
- [Beneš-UF-*et al.* 14] Structural Refinement for the Modal nu-Calculus (ICTAC)
- [UF-Legay'14] The Quantitative Linear-Time–Branching-Time Spectrum (Theor. Comput. Sci)
- [Bujtor-Vogler'15] Failure Semantics for Modal Transition Systems (ACM Trans. Embedded Comput. Syst.)