General Quantitative Specification Theories (with Modalities)

Sebastian S. Bauer Uli Fahrenberg Axel Legay Claus Thrane

LMU München, Germany / IRISA Rennes, France / Aalborg University, Denmark

CSR, July 2012

Upshot

Specification theory: (*cf.* [Bauer-David-Hennicker-Larsen-Legay-Nyman-Wąsowski–FASE'12])

- class of specifications $\mathcal{S}$
- satisfaction / refinement relation $\leq$
- parallel composition
  - $S \leq T \wedge S' \leq T' \Longrightarrow S \| S' \leq T \| T'$
- quotient
  - $\forall X \in \mathcal{S} : S \| X \leq T \Longleftrightarrow X \leq T \setminus\!\!\setminus S$
- conjunction
  - $\forall X \in \mathcal{S} : X \leq S \wedge T \Longleftrightarrow X \leq S \wedge X \leq T$

What if refinement is *quantitative* ?

- instead of relation $\leq \subseteq \mathcal{S} \times \mathcal{S}$, a distance $\mathcal{S} \times \mathcal{S} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$
- what are the defining properties of operations ?
- what are useful properties of operations ?

Structured Modal Transition Systems

Spec: set of specification labels with partial order $\sqsubseteq$

- denoting refinement of labels

$\mathsf{Imp} = \{k \in \mathsf{Spec} \mid k' \sqsubseteq k \implies k' = k\}$: set of implementation labels

Definition: Structured modal transition system

A SMTS is a tuple $(S, s^0, \dashrightarrow, \longrightarrow)$ with

- S: set of states, $s^0 \in S$,
- $\longrightarrow, \dashrightarrow \subseteq S \times \mathsf{Spec} \times S$,
- for all $s \xrightarrow{k} s'$ there is $s \overset{\ell}{\dashrightarrow} s'$ with $k \sqsubseteq \ell$.

Definition: Implementation

A SMTS is an implementation if $\longrightarrow = \dashrightarrow \subseteq S \times \mathsf{Imp} \times S$.

Refinement Distance

Old definition:

Modal refinement: relation $d_m : S_1 \times S_2 \to \{0,1\}$: greatest fixed point to

$$d_m(s_1, s_2) = \min \begin{cases} \forall s_1 \overset{k}{\dashrightarrow}_1 t_1 : \exists s_2 \overset{k}{\dashrightarrow}_2 t_2 : d_m(t_1, t_2) = 1\,, \\ \forall s_2 \overset{k}{\longrightarrow}_2 t_2 : \exists s_1 \overset{k}{\longrightarrow}_1 t_1 : d_m(t_1, t_2) = 1\,. \end{cases}$$

New definition

Modal refinement distance $d_m : S_1 \times S_2 \to \mathbb{L}$: least fixed point to

$$d_m(s_1, s_2) = \max \begin{cases} \sup\limits_{s_1 \overset{k_1}{\dashrightarrow}_1 t_1} \inf\limits_{s_2 \overset{k_2}{\dashrightarrow}_2 t_2} F(k_1, k_2, d_m(t_1, t_2))\,, \\ \sup\limits_{s_2 \overset{k_2}{\longrightarrow}_2 t_2} \inf\limits_{s_1 \overset{k_1}{\longrightarrow}_1 t_1} F(k_1, k_2, d_m(t_1, t_2))\,. \end{cases}$$

Distance Iterator

$\mathbb{L}$ and $F : \text{Spec} \times \text{Spec} \times \mathbb{L} \to \mathbb{L}$ come from [F.-Legay-Thrane-FSTTCS'11]:

- $\mathbb{L} = (\mathbb{R}_{\geq 0} \cup \{\infty\})^M$ (M some set): complete lattice with partial order $\sqsubseteq_{\mathbb{L}}$ and addition $\oplus_{\mathbb{L}}$
- F: distance iterator function which computes distances recursively.
- so *e.g.* for traces $k_0 k_1 \dots k_n$, $\ell_0 \ell_1 \dots \ell_m$:

$$d_T(k_0 k_1 \dots k_n, \ell_0 \ell_1 \dots \ell_m) = F(k_0, \ell_0, d_T(k_1 \dots k_n, \ell_1 \dots \ell_m))$$

- actual distances are obtained using a fixed lattice homomorphism $\mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\inf\}$
- axioms for $F(k, \ell, \alpha)$:
  - continuous in k and ℓ, monotone in α
  - $F(k, \ell, \alpha) = \sup_{k' \sqsubseteq k} \inf_{\ell' \sqsubseteq \ell} F(k', \ell', \alpha)$
  - $F(k, \ell, \alpha) \oplus_{\mathbb{L}} F(\ell, m, \beta) \sqsupseteq_{\mathbb{L}} F(k, m, \alpha \oplus_{\mathbb{L}} \beta)$

Structural Composition

Needs:

- partial label synchronization operator $\oplus$: Spec $\times$ Spec $\hookrightarrow$ Spec
- bound function $P : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ for which

$$F(k \oplus k', \ell \oplus \ell', P(\alpha, \alpha')) \sqsubseteq_{\mathbb{L}} P(F(k, \ell, \alpha), F(k', \ell', \alpha'))$$

Definition of structural composition is the standard one:

$$\frac{s \overset{k}{\dashrightarrow}_S s' \quad t \overset{\ell}{\dashrightarrow}_T t' \quad k \oplus \ell \text{ defined}}{(s, t) \overset{k \oplus \ell}{\dashrightarrow}_{S \| T} (s', t')} \qquad \frac{s \overset{k}{\longrightarrow}_S s' \quad t \overset{\ell}{\longrightarrow}_T t' \quad k \oplus \ell \text{ defined}}{(s, t) \overset{k \oplus \ell}{\longrightarrow}_{S \| T} (s', t')}$$

Theorem

$d_m(S \| S', T \| T') \sqsubseteq_{\mathbb{L}} P(d_m(S, T), d_m(S', T'))$

Quotient

Needs partial label operator $\oslash : \text{Spec} \times \text{Spec} \hookrightarrow \text{Spec}$ which is inverse to $\oplus$:

- for $k, \ell, m \in \text{Spec}$: $\ell \oslash k$ is defined and $m \sqsubseteq \ell \oslash k$ if and only if $k \oplus m$ is defined and $k \oplus m \sqsubseteq \ell$

Quantitative properties:

- good quotient: $F(m, \ell \oslash k, \alpha) \sqsupseteq_{\mathbb{L}} F(k \oplus m, \ell, \alpha)$ for all k, ℓ, m, α
- exact quotient: $F(m, \ell \oslash k, \alpha) = F(k \oplus m, \ell, \alpha)$ for all k, ℓ, m, α

Definition of quotient is the standard one (has to be!)

Theorem

Assume S deterministic and that $T \mathbin{\backslash\!\!\backslash} S$ exists.

- ***good:*** $d_m(X, T \mathbin{\backslash\!\!\backslash} S) \sqsupseteq d_m(S \| X, T)$
- ***exact:*** $d_m(X, T \mathbin{\backslash\!\!\backslash} S) = d_m(S \| X, T)$

Conjunction

Needs partial label conjunction operator $\oslash : \text{Spec} \times \text{Spec} \hookrightarrow \text{Spec}$

- lower bound: $k \oslash \ell \sqsubseteq k$ and $k \oslash \ell \sqsubseteq \ell$
- greatest lower bound: if $m \sqsubseteq k$ and $m \sqsubseteq \ell$, then $m \sqsubseteq k \oslash \ell$
- bounded: bound function $C : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ for which

$$F(m, k \oslash \ell, C(\alpha, \alpha')) \sqsubseteq_{\mathbb{L}} C(F(m, k, \alpha), F(m, \ell, \alpha'))$$

Definition of conjunction is the standard one (has to be!)

Theorem

- *If $\oslash$ is lower bound: $d_m(S \wedge T, S) = d_m(S \wedge T, T) = \bot_{\mathbb{L}}$.*
- *If $\oslash$ is greatest lower bound and S or T deterministic, then $d_m(U, S) = d_m(U, T) = \bot_{\mathbb{L}}$ imply $d_m(U, S \wedge T) = \bot_{\mathbb{L}}$.*
- *If $\oslash$ is bounded and S or T deterministic, then $d_m(U, S \wedge T) \sqsubseteq_{\mathbb{L}} C(d_m(U, S), d_m(U, T))$.*

- $\mathsf{Spec} = \Sigma \times \{[x,y] \mid x \in \mathbb{Z} \cup \{-\infty\}, y \in \mathbb{Z} \cup \{\infty\}\}$
- $d((a,[l,r]),(a,[l',r'])) = \max_{x\in[l,r]} \min_{x'\in[l',r']} |x - x'| = \max(0, l' - l, r - r')$

[Bauer-F.-Juhl-Larsen-Legay-Thrane–MFCS'11]:

- $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$, $F(k,\ell,\alpha) = d(k,\ell) + \lambda\alpha$ (accumulating distance)
- $(a,[l,r]) \oplus (a,[l',r']) = (a,[l+l',r+r'])$: bounded by $P(x,x') = x + x'$; exact quotient
- $(a,[l,r]) \owedge (a,[l',r']) = (a,[\max(l,l'),\min(r,r')])$: not bounded!

More useful for real-time systems:

- $\mathbb{L} = (\mathbb{R}_{\geq 0} \cup \{\infty\}^{\mathbb{R}}$, $F(k,\ell,\alpha)(\delta) = \max(|\delta + d'(k,\ell)|, \alpha(\delta + d'(k,\ell)))$ (max-lead distance)
- $k \oplus \ell = k \owedge \ell$ (intersection): bounded by $P(x,x') = \max(x,x')$; good quotient
- conjunction not bounded

Relaxed Conjunction

What to do if conjunction is not bounded?

- typical reason: may have $d(m,k) \neq \infty$ and $d(m,\ell) \neq \infty$, but $k \oslash \ell$ empty!
- idea: systematic widening of labels: if $d(m,k) \neq \infty$ and $d(m,\ell) \neq \infty$, then there are $k' \sqsupseteq k$ and $\ell' \sqsupseteq \ell$ with $k' \oslash \ell'$ non-empty

Theorem

Let S, T be SMTS with S or T deterministic and $\oslash$ relaxed conjunctively bounded by C. If there is an SMTS U for which $d_m(U,S), d_m(U,T) \neq \top_{\mathbb{L}}$, then there exist β- and γ-widenings S' of S and T' of T for which $S' \wedge T'$ is defined, and such that $d_m(U, S' \wedge T') \sqsubseteq_{\mathbb{L}} C_{\beta,\gamma}(d_m(U,S), d_m(U,T))$ for all SMTS U for which $d_m(U,S) \neq \top_{\mathbb{L}}$ and $d_m(U,T) \neq \top_{\mathbb{L}}$.

- Works for both examples.