Quantitative Refinement for Weighted Modal Transition Systems

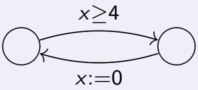
Sebastian S. Bauer Uli Fahrenberg Line Juhl Kim G. Larsen
Axel Legay Claus Thrane

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

MFCS 2011

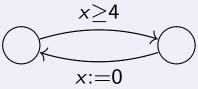
Quantitative Analysis

Quantitative *Models*



Quantitative Quantitative Analysis

Quantitative *Models*

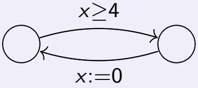


Quantitative *Specifications*

$$\Pr_{\leq .1}(\Diamond \mathit{error})$$

Quantitative Quantitative Quantitative Analysis

Quantitative *Models*



Quantitative *Specifications*

$\mathrm{Pr}_{\leq .1}(\Diamond error)$

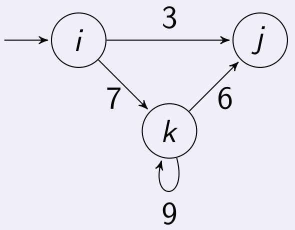
Quantitative *Verification*

$[\![\phi]\!](s) = 3.14$

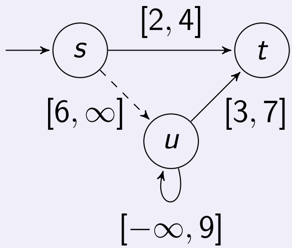
$d(s, t) = 42$

Examples

A quantitative *model*



A quantitative *specification*

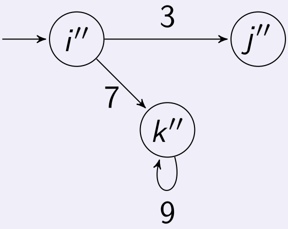


- Models: integer-weighted transition systems
- Specifications: integer-interval-weighted *modal* transition systems
  - *must*-transitions: must be implemented
  - *may*-transitions: can be present in implementations
- i is an implementation of s

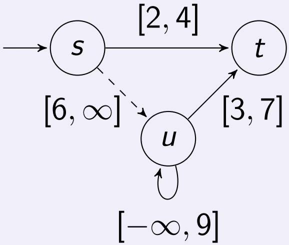
Examples

Another model

And another one



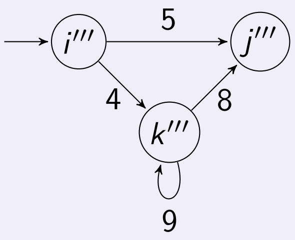
The specification



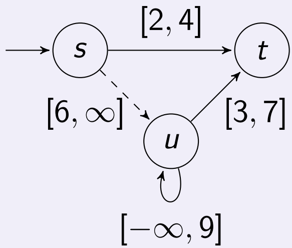
- i' is an implementation of s
- but i'' is not

Examples

Yet another model



The specification



- i''' is not an implementation of s
- (some of the weights are slightly off)
- but maybe it's close enough?

Definitions

Let $\mathbb{I} = \{[x, y] \mid x \in \mathbb{Z} \cup \{-\infty\}, y \in \mathbb{Z} \cup \{\infty\}, x \leq y\}$: the set of closed extended-integer intervals

Definition: Weighted modal transition system

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

- S: set of states, $s^0 \in S$,
- $\longrightarrow \subseteq \dashrightarrow \subseteq S \times \mathbb{I} \times S$.

Definition: Implementation

A WMTS is an implementation if $\longrightarrow \subseteq \dashrightarrow \subseteq S \times \mathbb{Z} \times S$.

Definitions

For intervals $k_1 = [l_1, r_1]$, $k_2 = [l_2, r_2]$ let

$$d(k_1, k_2) = \sup_{x_1 \in k_1} \inf_{x_2 \in k_2} |x_1 - x_2| = \max(0, l_2 - l_1, r_1 - r_2)$$

Also, λ with $0 < \lambda < 1$ is a discounting factor.

Definition: Modal refinement distance

Let S_1, S_2 be WMTS. The *modal refinement distance* $d_m : S_1 \times S_2 \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ is the least fixed point to the equations

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

Also, $d_m(S_1, S_2) = d_m(s_1^0, s_2^0)$.

Definitions

Hence:

- $d_m(I_1, I_2)$: how far are I_1 and I_2 from being bisimilar
- $d_m(I_1, S_2)$: how far is I_1 from being an implementation of S_2
- $d_m(S_1, S_2)$ measures the quantitative differences in the two specifications

Also, thorough refinement distance:

$$d_t(S_1, S_2) = \sup_{d_m(I_1, S_1)=0} \inf_{d_m(I_2, S_2)=0} d_m(I_1, I_2)$$

- $d_t(S_1, S_2)$ measures the (asymmetric Hausdorff) difference between the sets of implementations
- $d_t \leq d_m$, and $=$ for *deterministic* specifications

Transitivity

Note the triangle inequality:

$$d_m(S, U) \leq d_m(S, T) + d_m(T, U)$$

Hence (with I in place of S)

- if I is an almost-implementation of T
- and T is closely related to U
- then I is also an almost-implementation of U

Structural Composition

Goal: Composition operator $\|$ on specifications such that

- if I_1 is an almost-implementation of S_1
- and I_2 is an almost-implementation of S_2
- then $I_1 \| I_2$ is an almost-implementation of $S_1 \| S_2$.

Structural Composition

We use addition of weights when synchronizing:

$$[l_1, r_1] \oplus [l_2, r_2] = [l_1 + l_2, r_1 + r_2]$$

Definition: Structural composition

$S_1 \| S_2 = \big(S_1 \times S_2, (s_1^0, s_2^0), \mathrm{Spec}, \dashrightarrow, \longrightarrow\big)$ with

$$\frac{s_1 \overset{k_1}{\dashrightarrow}_1 t_1 \quad s_2 \overset{k_2}{\dashrightarrow}_2 t_2}{(s_1, s_2) \overset{k_1 \oplus k_2}{\dashrightarrow} (t_1, t_2)} \qquad \frac{s_1 \xrightarrow{k_1}_1 t_1 \quad s_2 \xrightarrow{k_2}_2 t_2}{(s_1, s_2) \xrightarrow{k_1 \oplus k_2} (t_1, t_2)}$$

Theorem

$d_m\big(S_1 \| S_3, S_2 \| S_4\big) \leq d_m(S_1, S_2) + d_m(S_3, S_4)$

Quotient

Goal: Quotient operator $\setminus\!\!\setminus$ on specifications such that

- for any almost-implementation I of S,
- J is an almost-implementation of $T \setminus\!\!\setminus S$
- iff $I \| J$ is an almost-implementation of T.

Property of quotient

For all specifications X: $d_m(S \| X, T) = d_m(X, T \setminus\!\!\setminus S)$

Quotient

A partial inverse to $\oplus$:

$$[l_1, r_1] \ominus [l_2, r_2] = \begin{cases} [l_1 - l_2, r_1 - r_2] & \text{if } l_1 - l_2 \leq r_1 - r_2 \\ \text{undefined} & \text{otherwise} \end{cases}$$

Definition: Quotient

$$S_1 \mathbin{\backslash\!\!\backslash} S_2 = \big(S_1 \times S_2 \cup \{u\}, (s_1^0, s_2^0), \text{Spec}, \dashrightarrow, \longrightarrow\big) \text{ with}$$

$$\frac{s_1 \overset{k_1}{\dashrightarrow}_1 t_1 \quad s_2 \overset{k_2}{\dashrightarrow}_2 t_2 \quad k_1 \ominus k_2 \text{ def.}}{(s_1, s_2) \overset{k_1 \ominus k_2}{\dashrightarrow} (t_1, t_2)} \qquad \frac{s_1 \overset{k_1}{\longrightarrow}_1 t_1 \quad s_2 \overset{k_2}{\longrightarrow}_2 t_2 \quad k_1 \ominus k_2 \text{ def.}}{(s_1, s_2) \overset{k_1 \ominus k_2}{\longrightarrow} (t_1, t_2)}$$

$$\frac{s_1 \overset{k_1}{\longrightarrow}_1 t_1 \quad \forall s_2 \overset{k_2}{\longrightarrow}_2 t_2 : k_1 \ominus k_2 \text{ undef.}}{(s_1, s_2) \text{ bad}}$$

$$\frac{k \in \text{Spec} \quad \forall s_2 \overset{k_2}{\dashrightarrow}_2 t_2 : k \oplus k_2 \text{ undef.}}{(s_1, s_2) \overset{k}{\dashrightarrow} u} \qquad \frac{k \in \text{Spec}}{u \overset{k}{\dashrightarrow} u}$$

and then remove bad states and states which *must* lead to them.

Conjunction

Goal: Conjunction operator $\wedge$ on specifications such that

- I is an almost-implementation of S_1 and of S_2
- iff I is an almost-implementation of $S_1 \wedge S_2$.

Conjunction as greatest lower bound

$d_m(S_1 \wedge S_2, S_1) = d_m(S_1 \wedge S_2, S_2) = 0$, and
if $d_m(S, S_1) = 0$ and $d_m(S, S_2) = 0$, then also $d_m(S, S_1 \wedge S_2) = 0$.

This implies uniqueness: if conjunction exists, it is unique.

Also want continuity:
$\forall \varepsilon . \exists \varepsilon_1, \varepsilon_2 . d_m(S, S_1) \leq \varepsilon_1$ and $d_m(S, S_2) \leq \varepsilon_2$ imply $d_m(S, S_1 \wedge S_2) \leq \varepsilon$

Theorem

No such conjunction exists.

Conclusion

- For quantitative specification theories,
- precise notions of refinement are useless.
- Instead, need to consider refinement distances.

- Operations (composition, quotient, conjunction, ...) should be continuous:
- small refinement distances are preserved.

- For our example of WMTS,
- composition and quotient work nicely,
- but conjunction does not. (This can be fixed though.)

Commercial Break

FORMATS 2011

9th International Conference on Formal Modeling and Analysis of Timed Systems