Reasoning About Bounds In Weighted Transition Systems

QuantLA 2017

September 18, 2017

Mikkel Hansen, Kim Guldstrand Larsen, Radu Mardare,
Mathias Ruggaard Pedersen and Bingtian Xue
{mhan, kgl, mardare, mrp, bingt}@cs.aau.dk

Department of Computer Science
Aalborg University
Denmark

AALBORG UNIVERSITY
DENMARK

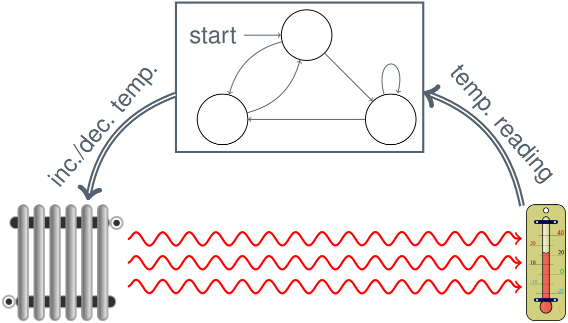
Slides adapted from Mikkel Hansen

Introduction

Introduction

Background

Cyber-Physical Systems operate in environments that are inherently unpredictable and imprecise.



Introduction

Motivation

Observation

- When modeling physical phenomena, their quantitative nature is most often captured by means of observations and measurements.
- The accuracy of these measurements is highly dependent on the methods/equipment used to obtain them as well as the environment in which they are obtained.

Introduction

Motivation

Observation

- When modeling physical phenomena, their quantitative nature is most often captured by means of observations and measurements.
- The accuracy of these measurements is highly dependent on the methods/equipment used to obtain them as well as the environment in which they are obtained.

Example

Consider measuring some physical phenomena with a piece of equipment that is known to be accurate within one unit.

Introduction

Motivation

Example

Consider measuring some physical phenomena with a piece of equipment that is known to be accurate within one unit.

We may obtain a reading of x and thus conclude that the actual value is somewhere in the interval $[x - 1; x + 1]$.

Introduction

Motivation

Example

Consider measuring some physical phenomena with a piece of equipment that is known to be accurate within one unit.

We may obtain a reading of x and thus conclude that the actual value is somewhere in the interval $[x - 1; x + 1]$.

Problem

What quantity should we use in our model?

Introduction

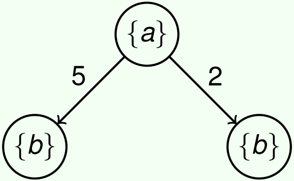
Motivation

Problem

What quantity should we use in our model?

Solution 1: Naive Approach

Use the concrete value *x* regardless of the possible inaccuracy of the measurement.



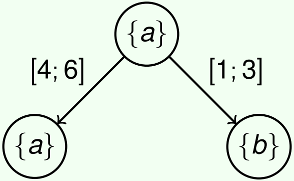
Introduction

Motivation

Solution 2: Abstractions

Realize the inherent uncertainty in the quantitative measures and try to abstract it away in the models.

In our example, a natural solution could be to use the interval $[x - 1; x + 1]$ as a quantitative measure.



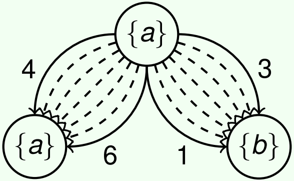
The model then describes how the system can or may be implemented.

Introduction

Motivation

Our Approach

We abstract away the intermediate transitions in $[x-1; x+1]$,

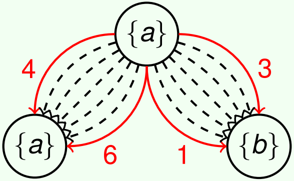


Introduction

Motivation

Our Approach

We abstract away the intermediate transitions in $[x - 1; x + 1]$,



and instead reason only about the lower/upper bounds on transition weights.

Introduction

Contribution

Our Contribution

- Reasoning about min and max transitions, including bisimulation.

Introduction

Contribution

Our Contribution

- Reasoning about min and max transitions, including bisimulation.
- Modal logic that is invariant under bisimulation.

Introduction

Contribution

Our Contribution

- Reasoning about min and max transitions, including bisimulation.
- Modal logic that is invariant under bisimulation.
- Finite model property and satisfiability checking algorithm.

Introduction

Contribution

Our Contribution

- Reasoning about min and max transitions, including bisimulation.
- Modal logic that is invariant under bisimulation.
- Finite model property and satisfiability checking algorithm.
- Complete axiomatization for the logic.

Models

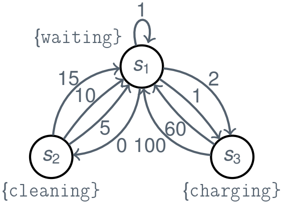
Model

Weighted Transition Systems

Definition: Weighted Transition System

A weighted transition system (WTS) is a tuple $\mathcal{M} = (S, \rightarrow, \ell)$, where

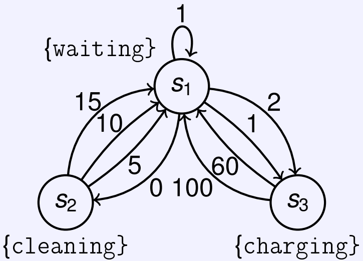
- S is a non-empty set of *states*,
- $\rightarrow \subseteq S \times \mathcal{R}_{\geq 0} \times S$ is the *transition relation*, and
- $\ell : S \rightarrow 2^{AP}$ is a *labeling function* mapping to each state a set of atomic propositions.



Model

Example: Robot Vacuum Cleaner

Example: A model of a robot vacuum cleaner



3 states: `waiting`, `cleaning` and `charging`.

The time it takes to move between states is given by the transition weights.

Model

Image Sets

Definition: Image Set

For arbitrary WTS $\mathcal{M} = (S, \rightarrow, \ell)$ the function

$$\theta : S \rightarrow (2^{S} \rightarrow 2^{\mathcal{R}_{\geq 0}})$$

is defined for any state $s \in S$ and any set of states $T \subseteq S$ as

$$\theta = \left\{ x \in \mathcal{R}_{\geq 0} \mid \exists t \in T \text{ such that } s \xrightarrow{x} t \right\}$$

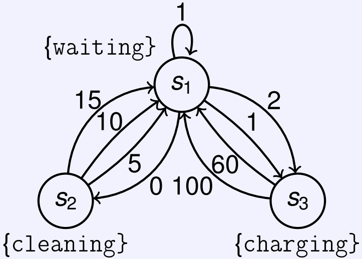
We refer to $\theta(s)(T)$ as the *image* from s to T or simply an *image set*.

$$\theta^{-}(s)(T) = \inf \theta(s)(T) \quad \text{and} \quad \theta^{+}(s)(T) = \sup \theta(s)(T)$$

Model

Example: Robot Vacuum Cleaner

Example: A model of a robot vacuum cleaner



$\theta(s_1)(\{s_2\}) = \{0\}$

$\theta(s_2)(\{s_1\}) = \{5, 10, 15\}$

$\theta^-(s_1)(\{s_2\}) = 0$

$\theta^-(s_2)(\{s_1\}) = 5$

$\theta^+(s_1)(\{s_2\}) = 0$

$\theta^+(s_2)(\{s_1\}) = 15$

Model

Bisimulation

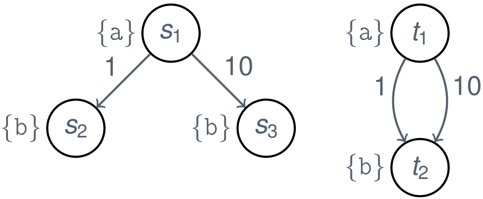
Definition: Weighted Bisimilarity $\sim_W$

Given a WTS $\mathcal{M} = (S, \rightarrow, \ell)$, a binary relation $\mathcal{R}$ on S is called a *weighted bisimulation relation* if and only if $s\mathcal{R}t$ implies

(Atomic Harmony) $\ell(s) = \ell(t)$,

(Zig) $s \xrightarrow{x} s'$ implies $t \xrightarrow{x} t'$ such that $s'\mathcal{R}t'$, and

(Zag) $t \xrightarrow{x} t'$ implies $s \xrightarrow{x} s'$ such that $s'\mathcal{R}t'$.



$$\mathcal{R} = \left\{ \begin{array}{ll} (s_1, t_1), & (t_1, s_1), \\ (s_2, t_2), & (t_2, s_2), \\ (s_3, t_2), & (t_2, s_3), \\ (s_2, s_3), & (s_3, s_2) \end{array} \right\}$$

is a bisimulation relation

Model
Bisimulation

Definition: Generalized Weighted Bisimilarity $\sim$

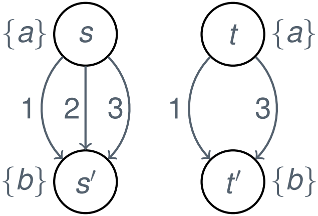
Given a WTS $\mathcal{M} = (S, \rightarrow, \ell)$, an equivalence relation $\mathcal{R}$ on S is called a *generalized weighted bisimulation* iff $s\mathcal{R}t$ implies

(Atomic Harmony) $\ell(s) = \ell(t)$,

(Lower Bound) $\theta^-(s)(T) = \theta^-(t)(T)$, and

(Upper Bound) $\theta^+(s)(T) = \theta^+(t)(T)$

for any $\mathcal{R}$-equivalence class $T \in S/\mathcal{R}$.



$\theta^-(s)(\{s', t'\}) = \theta^-(t)(\{s', t'\})$
and
$\theta^+(s)(\{s', t'\}) = \theta^+(t)(\{s', t'\})$
so
$s \sim t$ but $s \not\sim_W t$

Model
Bisimulation

Theorem: Relation between $\sim$ and $\sim_W$

Generalized weighted bisimilarity is coarser than weighted bisimilarity, i.e.

$$\sim_W \subsetneq \sim$$

Logic

Logic

Syntax and Semantics

Definition: Syntax of $\mathcal{L}$

$$\mathcal{L}: \quad \varphi, \psi ::= p \mid \neg\varphi \mid \varphi \wedge \psi \mid L_r\varphi \mid M_r\varphi$$

Definition: L_r and M_r Semantics

$$\mathcal{M}, s \models L_r\varphi \quad \text{iff} \quad \theta^-(s)(\llbracket\varphi\rrbracket) \geq r$$

$$\mathcal{M}, s \models M_r\varphi \quad \text{iff} \quad \theta^+(s)(\llbracket\varphi\rrbracket) \leq r$$

where $\llbracket\varphi\rrbracket = \{t \in S \mid \mathcal{M}, t \models \varphi\}$.

Logic

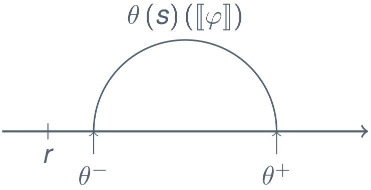
Syntax and Semantics

Definition: L_r and M_r Semantics

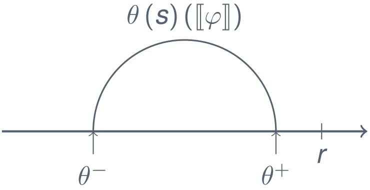
$$\mathcal{M}, s \models L_r\varphi \quad \text{iff} \quad \theta^-(s)(\llbracket\varphi\rrbracket) \geq r$$

$$\mathcal{M}, s \models M_r\varphi \quad \text{iff} \quad \theta^+(s)(\llbracket\varphi\rrbracket) \leq r$$

where $\llbracket\varphi\rrbracket = \{t \in S \mid \mathcal{M}, t \models \varphi\}$.



(a) $\mathcal{M}, s \models L_r\varphi$

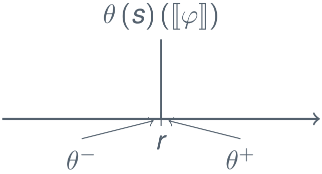


(b) $\mathcal{M}, s \models M_r\varphi$

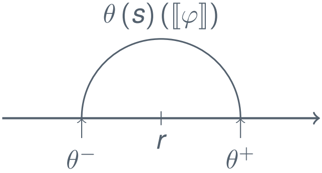
Logic

Syntax and Semantics

It is possible that $L_r\varphi$ and $M_r\varphi$ are both satisfied at the same time.



This also holds for their negation, $\neg L_r\varphi$ and $\neg M_r\varphi$.



Logic

Bisimulation Invariance

Theorem: Bisimulation Invariance

For any image-finite WTS $\mathcal{M} = (S, \rightarrow, \ell)$ and states $s, t \in S$ it holds that

$$s \sim t \quad \text{iff} \quad [\forall \varphi \in \mathcal{L}.\ \mathcal{M}, s \models \varphi \text{ iff } \mathcal{M}, t \models \varphi]$$

Metatheory

Metatheory

Axioms

(A1):	$\vdash \neg L_0 \bot$	
(A2):	$\vdash L_{r+q}\varphi \to L_r\varphi$	if $q > 0$
(A2′):	$\vdash M_r\varphi \to M_{r+q}\varphi$	if $q > 0$
(A3):	$\vdash L_r\varphi \wedge L_q\psi \to L_{\min\{r,q\}}(\varphi \vee \psi)$	
(A3′):	$\vdash M_r\varphi \wedge M_q\psi \to M_{\max\{r,q\}}(\varphi \vee \psi)$	
(A4):	$\vdash L_r(\varphi \vee \psi) \to L_r\varphi \vee L_r\psi$	
(A5):	$\vdash \neg L_0\psi \to (L_r\varphi \to L_r(\varphi \vee \psi))$	
(A5′):	$\vdash \neg L_0\psi \to (M_r\varphi \to M_r(\varphi \vee \psi))$	
(A6):	$\vdash L_{r+q}\varphi \to \neg M_r\varphi$	if $q > 0$
(A7):	$\vdash M_r\varphi \to L_0\varphi$	
(R1):	$\vdash \varphi \to \psi \implies \vdash ((L_r\psi) \wedge (L_0\varphi)) \to L_r\varphi$	
(R1′):	$\vdash \varphi \to \psi \implies \vdash ((M_r\psi) \wedge (L_0\varphi)) \to M_r\varphi$	
(R2):	$\vdash \varphi \to \psi \implies \vdash L_0\varphi \to L_0\psi$	

Metatheory

Axioms

(A1): $\vdash \neg L_0 \bot$

(A2): $\vdash L_{r+q}\varphi \rightarrow L_r\varphi$ if $q > 0$

(A2′): $\vdash M_r\varphi \rightarrow M_{r+q}\varphi$ if $q > 0$

(A3): $\vdash L_r\varphi \wedge L_q\psi \rightarrow L_{\min\{r,q\}}(\varphi \vee \psi)$

(A3′): $\vdash M_r\varphi \wedge M_q\psi \rightarrow M_{\max\{r,q\}}(\varphi \vee \psi)$

(A4): $\vdash L_r(\varphi \vee \psi) \rightarrow L_r\varphi \vee L_r\psi$

(A5): $\vdash \neg L_0\psi \rightarrow (L_r\varphi \rightarrow L_r(\varphi \vee \psi))$

(A5′): $\vdash \neg L_0\psi \rightarrow (M_r\varphi \rightarrow M_r(\varphi \vee \psi))$

(A6): $\vdash L_{r+q}\varphi \rightarrow \neg M_r\varphi$ if $q > 0$

(A7): $\vdash M_r\varphi \rightarrow L_0\varphi$

(R1): $\vdash \varphi \rightarrow \psi \implies \vdash ((L_r\psi) \wedge (L_0\varphi)) \rightarrow L_r\varphi$

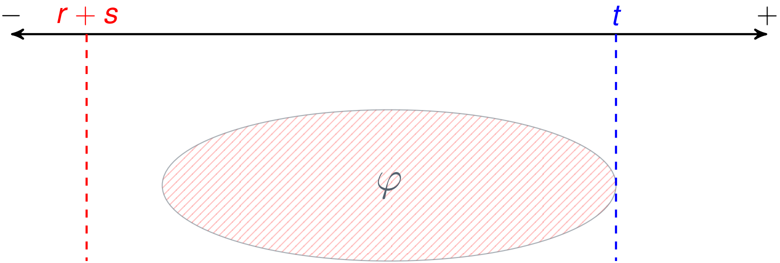
(R1′): $\vdash \varphi \rightarrow \psi \implies \vdash ((M_r\psi) \wedge (L_0\varphi)) \rightarrow M_r\varphi$

(R2): $\vdash \varphi \rightarrow \psi \implies \vdash L_0\varphi \rightarrow L_0\psi$

Metatheory

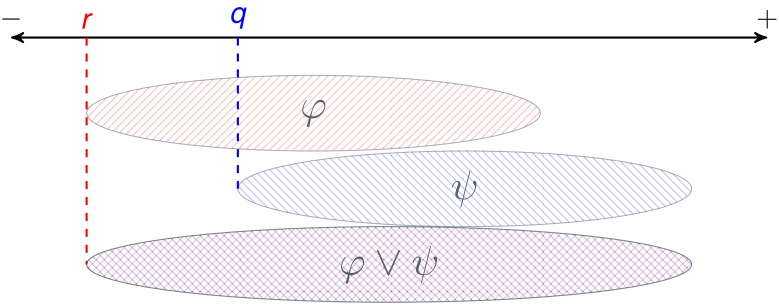
A2 and A2'

(A2) $\vdash L_{r+s}\varphi \to L_r\varphi,\ s > 0$ **(A2')** $\vdash M_t\varphi \to M_{t+q}\varphi,\ q > 0$



Metatheory
A3

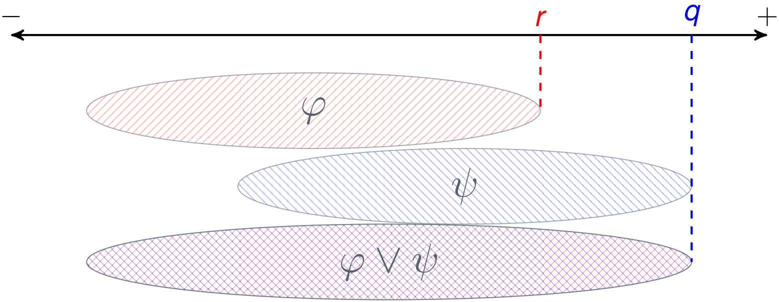
(A3) $\vdash L_r\varphi \wedge L_q\psi \rightarrow L_{\min\{r,q\}}(\varphi \vee \psi)$



Metatheory

A3’

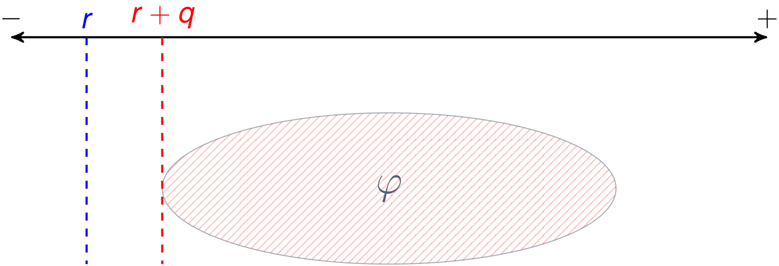
(A3’) $\vdash M_r\varphi \wedge M_q\psi \rightarrow M_{\max\{r,q\}}(\varphi \vee \psi)$



Metatheory

A6

(A8) $\vdash L_{r+q}\varphi \rightarrow \neg M_r\varphi, q > 0$

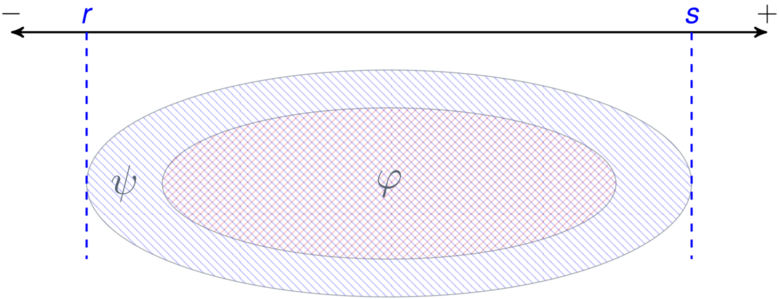


Metatheory

R1 and R1'

$$\textbf{(R1)} \quad \vdash \varphi \to \psi \implies ((L_r\psi) \wedge (L_0\varphi)) \to L_r\varphi$$

$$\textbf{(R1')} \quad \vdash \varphi \to \psi \implies ((M_s\psi) \wedge (L_0\varphi)) \to M_s\varphi$$



Metatheory

Soundness

Lemma: Soundness

$\vdash \varphi$ implies $\models \varphi$

Metatheory

Finite Model Construction

Starting from a *consistent* formula $\varphi \in \mathcal{L}$, we do the following based on φ

1. Construct a finite subset $\mathcal{L}[\varphi]$ of $\mathcal{L}$
2. Construct a model $\mathcal{M}_\varphi$ where:
   - States are the maximal consistent sets (ultrafilters) of $\mathcal{L}[\varphi]$
   - Transitions are given by the formulae in these sets, i.e. $L_r\varphi \in u$ implies $u \xrightarrow{x} [\![\varphi]\!]$ where $x \geq r$.

Then, $\mathcal{M}_\varphi$ is a model for φ.

Metatheory

Finite Model Property

Lemma: Truth Lemma

If $\varphi \in \mathcal{L}$ is a consistent formula, then for formulae all $\psi \in \mathcal{L}[\varphi]$ and ultrafilters $u \subseteq \mathcal{L}[\varphi]$ we have

$$\mathcal{M}_\varphi, u \models \psi \quad \text{iff} \quad \psi \in u$$

Lemma: Finite Model Property

For any consistent formula $\varphi \in \mathcal{L}$, there exists a finite WTS $\mathcal{M} = (S, \rightarrow, \ell)$ and a state $s \in S$ such that

$$\mathcal{M}, s \models \varphi$$

Metatheory

Completeness

Theorem: Completeness

For any formula $\varphi \in \mathcal{L}$ it holds that

$$\models \varphi \quad \text{implies} \quad \vdash \varphi$$

Conclusions

Concluding Remarks

We have proposed abstracting away individual transition weights in a WTS by introducing the notion of an *image set*.

We have proposed a modal logic that reasons about the minimum and maximum weights on transitions and shown that it has the finite model property.

We have presented a procedure for determining the satisfiability of formulae in our logic (not covered in this talk).

We have proposed an axiomatization for our logic and shown that is is complete.

Open Problems

Open Problems
Strong Completeness

There is a stronger notion of completeness, often called *strong completeness*, which asserts that $\Phi \models \varphi$ implies $\Phi \vdash \varphi$ for any set of formulae $\Phi \subseteq \mathcal{L}$.

Completeness is a special case of strong completeness where $\Phi = \emptyset$.

In the case of compact logics, strong completeness follows directly from completeness. However, our logic is non-compact.

$$\Phi = \{L_q\varphi \mid q < r\} \cup \{\neg L_r\varphi\}$$

Open Problems

Temporal Specification

Many interesting properties of CPSs such as *liveness* and *deadlock freeness* cannot be expressed in modal logic.

We would like to explore temporal specification languages such as *CTL* or *LTL*.

Thank you