A Complete Approximation Theory for Weighted Transition Systems

December 1, 2015

Peter Christoffersen Mikkel Hansen **Mathias R. Pedersen**
Radu Mardare Kim G. Larsen

Department of Computer Science
Aalborg University
Denmark

AALBORG UNIVERSITY
DENMARK

Agenda

Introduction

Logic

Axiomatization

Canonical model construction

Weak completeness

Conclusion

Motivation

Today microchips are used nearly everywhere we look.

Cyber-physical systems

The idea of combining computation and the physical world.

- Use sensors and input devices for humans to affect the computation.
- Motors, actuators and other mechanics can alter and affect the world.

Motivation

Today microchips are used nearly everywhere we look.

Cyber-physical systems

The idea of combining computation and the physical world.

- Use sensors and input devices for humans to affect the computation.
- Motors, actuators and other mechanics can alter and affect the world.

When dealing with real-world processes you often rely on resources such as:

- Energy, money, distances etc.

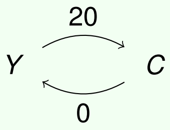
Motivation

Resource modeling

Weighted Transition Systems (WTS) can encode this quantitative behaviour, though in a strictly precise fashion.

WTS example: Robot vacuum cleaner

Clean? Yes.
Room is Cleaned.
The room takes 20 units, e.g. time or energy, to clean.



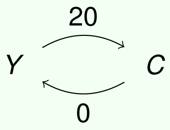
Motivation

Resource modeling

Weighted Transition Systems (WTS) can encode this quantitative behaviour, though in a strictly precise fashion.

WTS example: Robot vacuum cleaner

Clean? Yes.
Room is Cleaned.
The room takes 20 units, e.g. time or energy, to clean.



What if the room had a very varying degree of dirtiness?

Motivation
Resource modeling

Cyber-physical systems

Sensors and inputs from the world affects computations, likewise mechanical output affects the world.

The settings these systems operate in are often unpredictable, and the inputs are always with some imprecision.

Problems

- Tolerance of sensors.
- Unpredictable environment.

We can only reason about what is encoded in the model.

Motivation

Resource modeling

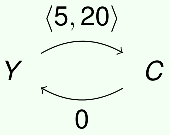
Solution

Let the model account for the imprecision so we can reason about it.

We extend the notion of WTS with bounds $\langle x, y \rangle$ on transitions.
This captures the imprecision in the modeling domain by denoting a whole range of values.

WTS example: Robot vacuum cleaner

Clean? Yes.
Room is Cleaned.
The room takes 5 to 20 units, e.g. time or energy, to clean.



Contribution

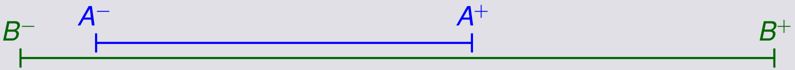
- An extension of Weighted Transition Systems with bounds, as well as a suitable notion of bisimulation.
- Logic to reason with bounds that has the Hennessy-Milner property.
- Weak-complete axiomatization of the logic.

Bounds

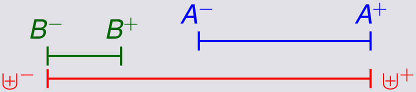
Bounds

A *bound* $B \in \mathbb{R}^2_{\geq 0}$ is either the empty set $\emptyset$ or a tuple $\langle x, y \rangle$ where $x \leq y$.
Denote the set of all bounds by $\mathfrak{B}$.

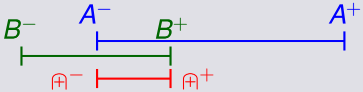
$A \sqsubseteq B$ iff $B^- \leq A^-$ and $A^+ \leq B^+$



$A \uplus B = \langle \min\{A^-, B^-\}, max\{A^+, B^+\} \rangle$



$A \mathbin{\cap\!\!\!\!+} B = \langle \max\{A^-, B^-\}, min\{A^+, B^+\} \rangle$



Generalized Weighted Transition Systems

A *Generalized Weighted Transition System (GTS)* is a tuple $\mathcal{G} = (S, \theta, \ell)$, where

Transition function

$\theta : S \to (2^S \to \mathfrak{B})$ is a *transition function* satisfying the following conditions:

$$\theta(s)(\emptyset) = \emptyset, \tag{I}$$

$$\theta(s)\left(\bigcup_i S_i\right) = \biguplus_i \theta(s)(S_i)\,, \text{ and} \tag{II}$$

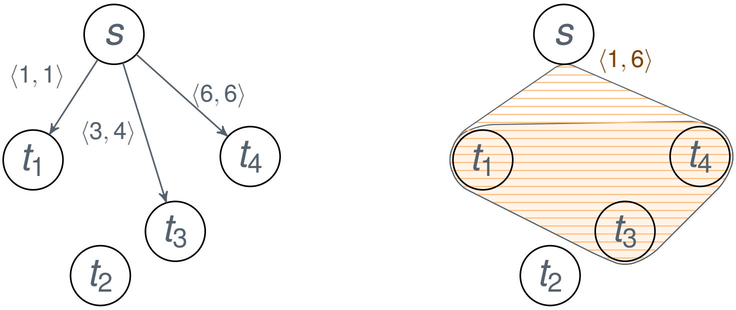
$$\theta(s)\left(\bigcap_i S_i\right) \neq \emptyset \implies \theta(s)\left(\bigcap_i S_i\right) = \bigoplus_i \theta(s)(S_i)\,. \tag{III}$$

GTS: Transition function

Property II

$$\theta(s)\left(\bigcup_i S_i\right) = \biguplus_i \theta(s)(S_i)$$

$$\theta(s)(\{t_1\} \cup \{t_3\} \cup \{t_4\}) = \langle \min\{1,3,6\}, \max\{1,4,6\} \rangle = \langle 1,6 \rangle$$



Logic
Syntax

Syntax

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

where $r \in \mathbb{Q}_{\geq 0}$ and $p \in \mathcal{AP}$.

Semantics

$\mathcal{G}, s \models L_r\varphi$ iff can reach a state satisfying φ with weight at least r

$\mathcal{G}, s \models M_r\varphi$ iff can reach a state satisfying φ with weight at most r

Logic
Syntax

Syntax

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

where $r \in \mathbb{Q}_{\geq 0}$ and $p \in \mathcal{AP}$.

Semantics

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

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

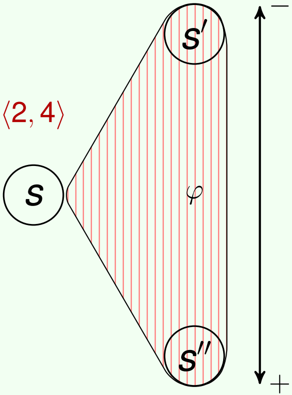
where $\llbracket\varphi\rrbracket$ is the set of all GTS states with the property φ, i.e.

$$\llbracket\varphi\rrbracket = \{s \mid \exists(S, \theta, \ell) \in \mathfrak{G} : s \in S \text{ and } \mathcal{G}, s \models \varphi\}$$

Logic

Example

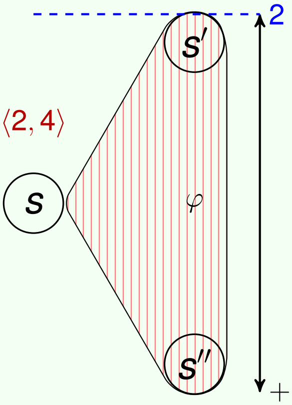
Example



Logic

Example

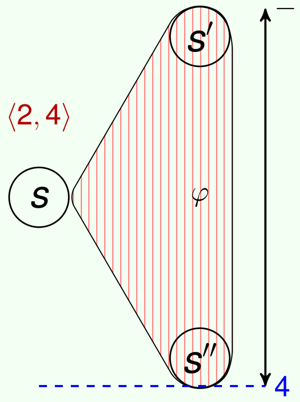
Example



$$\mathcal{G}, s \models L_2\varphi$$

Logic
Example

Example

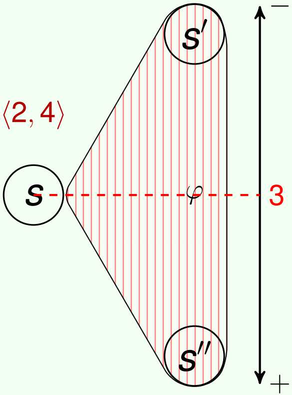


$$\mathcal{G}, s \models L_2\varphi$$

$$\mathcal{G}, s \models M_4\varphi$$

Logic
Example

Example



$\mathcal{G}, s \models L_2\varphi$

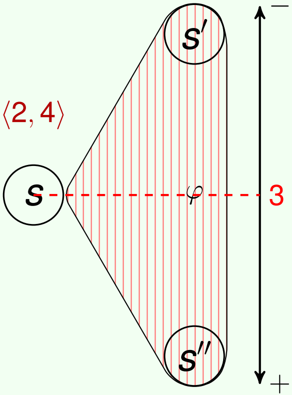
$\mathcal{G}, s \models M_4\varphi$

$\mathcal{G}, s \not\models L_3\varphi$

Logic

Example

Example



$\mathcal{G}, s \models L_2\varphi$

$\mathcal{G}, s \models M_4\varphi$

$\mathcal{G}, s \not\models L_3\varphi$

$\mathcal{G}, s \not\models M_3\varphi$

Logic
Derived operators

In addition to the operators defined by the syntax, we have the following derived operators

Derived operators

$$\bot \stackrel{\text{def}}{=} \varphi \wedge \neg\varphi \qquad \top \stackrel{\text{def}}{=} \neg\bot$$

$$\varphi \vee \psi \stackrel{\text{def}}{=} \neg(\neg\varphi \wedge \neg\psi) \qquad \varphi \to \psi \stackrel{\text{def}}{=} \neg\varphi \vee \psi$$

Logic
Derived operators

In addition to the operators defined by the syntax, we have the following derived operators

Derived operators

$$\bot \overset{\text{def}}{=} \varphi \land \neg\varphi \qquad \top \overset{\text{def}}{=} \neg\bot$$

$$\varphi \lor \psi \overset{\text{def}}{=} \neg(\neg\varphi \land \neg\psi) \qquad \varphi \to \psi \overset{\text{def}}{=} \neg\varphi \lor \psi$$

We can encode $\Box$ and $\Diamond$ with their usual semantics

$\Box$, $\Diamond$ semantics

$$\Diamond\varphi \overset{\text{def}}{=} L_0\varphi$$

$$\Box\varphi \overset{\text{def}}{=} \neg\Diamond\neg\varphi = \neg L_0\neg\varphi$$

Bisimulation

Bisimulation

Given GTS $\mathcal{G} = (S, \theta, \ell)$, an equivalence relation $\mathcal{R}$ on S is a bisimulation relation iff $s\mathcal{R}t$ implies

- $\ell(s) = \ell(t)$ and
- $\theta(s)(T) = \theta(t)(T)$ for all equivalence classes $T \in S/\mathcal{R}$.

Bisimulation invariance (Hennessy-Milner property)

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

Filters

Filter

A non-empty subset F of $\mathcal{L}$ is called a filter iff

- $\bot \notin F$,
- $\varphi \in F$ and $\vdash \varphi \to \psi$ implies $\psi \in F$, and
- $\varphi \in F$ and $\psi \in F$ implies $\varphi \wedge \psi \in F$.

Ultrafilter

A filter F is called an ultrafilter iff for every $\varphi \in \mathcal{L}$ either

$$\varphi \in F \quad \text{or} \quad \neg\varphi \in F,$$

but not both.

Axioms

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

(A2): $\vdash L_{r+s}\varphi \to L_r\varphi,\ s > 0$

(A2′): $\vdash M_r\varphi \to M_{r+s}\varphi,\ s > 0$

(A3): $\vdash L_r\varphi \wedge L_s\psi \to L_{\min\{r,s\}}(\varphi \vee \psi)$

(A3′): $\vdash M_r\varphi \wedge M_s\psi \to M_{\max\{r,s\}}(\varphi \vee \psi)$

(A4): $\vdash ((L_r\varphi) \wedge (L_s\psi)) \to (L_0\,(\varphi \wedge \psi) \to L_{\max\{r,s\}}\,(\varphi \wedge \psi))$

(A4′): $\vdash ((M_r\varphi) \wedge (M_s\psi)) \to (L_0\,(\varphi \wedge \psi) \to M_{\min\{r,s\}}\,(\varphi \wedge \psi))$

(A5): $\vdash ((L_0\varphi) \wedge (\neg L_r\varphi) \wedge (L_0\psi) \wedge (\neg L_s\psi)) \to \neg L_{\max\{r,s\}}\,(\varphi \wedge \psi)$

(A5′): $\vdash ((L_0\varphi) \wedge (\neg M_r\varphi) \wedge (L_0\psi) \wedge (\neg M_s\psi)) \to \neg M_{\min\{r,s\}}\,(\varphi \wedge \psi)$

(A6): $\vdash L_r(\varphi \vee \psi) \to L_r\varphi \vee L_r\psi$

(A6′): $\vdash M_r(\varphi \vee \psi) \to M_r\varphi \vee M_r\psi$

(A7): $\vdash \neg L_0\psi \to (L_r\varphi \to L_r(\varphi \vee \psi))$

(A7′): $\vdash \neg L_0\psi \to (M_r\varphi \to M_r(\varphi \vee \psi))$

(A8): $\vdash L_{r+s}\varphi \to \neg M_r\varphi,\ s > 0$

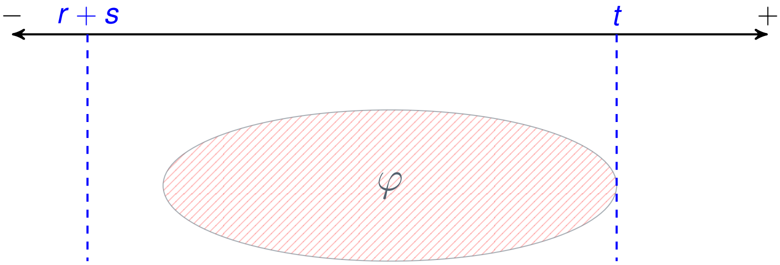
(A9): $\vdash M_r\varphi \to L_0\varphi$

Axioms

A2 and A2'

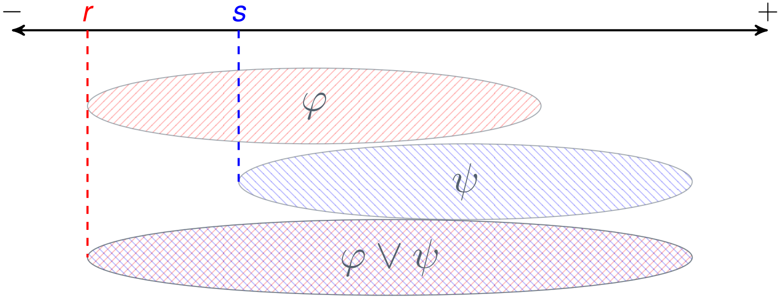
(A2) $\vdash L_{r+s}\varphi \rightarrow L_r\varphi, \; s > 0$

(A2') $\vdash M_t\varphi \rightarrow M_{t+q}\varphi, \; q > 0$



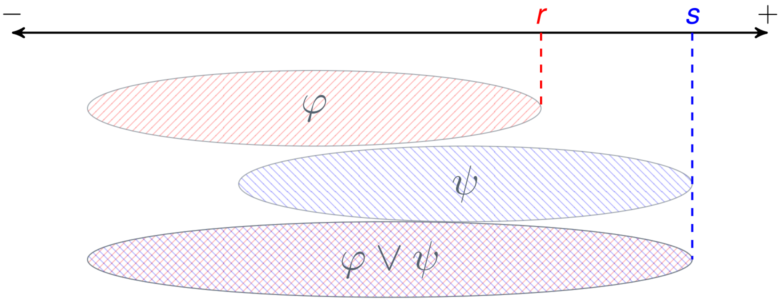
Axioms
A3

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



Axioms
A3'

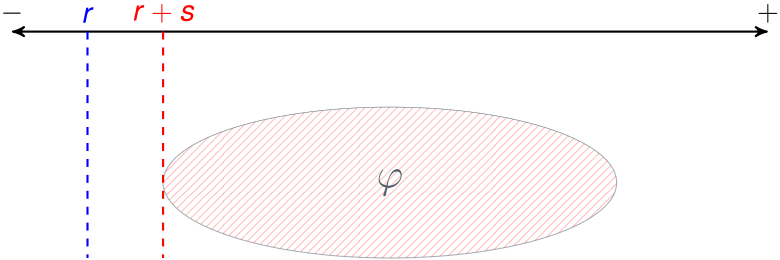
(A3') $\vdash M_r\varphi \wedge M_s\psi \rightarrow M_{\max\{r,s\}}(\varphi \vee \psi)$



Axioms

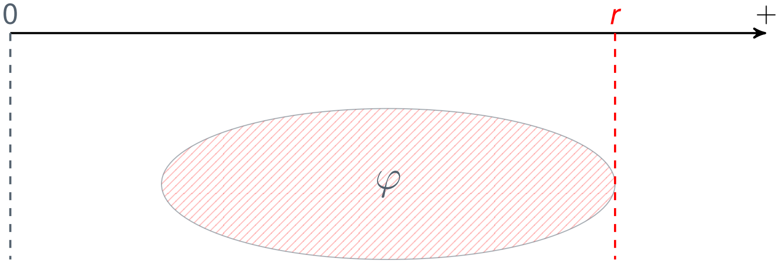
A8

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



Axioms
A9

(A9) $\vdash M_r\varphi \rightarrow L_0\varphi$



Axioms

(R1): $\{L_s\varphi \mid s < r\} \vdash L_r\varphi$

(R1′): $\{M_s\varphi \mid s > r\} \vdash M_r\varphi$

(R2): $\vdash \varphi \to \psi \implies \vdash ((L_r\psi) \wedge (L_0\varphi)) \to L_r\varphi$

(R2′): $\vdash \varphi \to \psi \implies \vdash ((M_s\psi) \wedge (L_0\varphi)) \to M_s\varphi$

(R3): $\vdash \varphi \to \psi \implies \vdash L_0\varphi \to L_0\psi$

(R4): $\{\neg M_r\varphi \mid r \in \mathbb{Q}_{\geq 0}\} \vdash \neg L_0\varphi$

(R5): $$\frac{\{\varphi_i \mid i \in \mathbb{N}\} \vdash \varphi \qquad \vdash \varphi_{i+1} \to \varphi_i \qquad \vdash \varphi \to \varphi_i \quad \forall i \in \mathbb{N}}{\{\neg L_r\varphi_i \mid i \in \mathbb{N}\} \vdash \neg L_{r+s}\varphi}, \quad s > 0$$

(R5′): $$\frac{\{\varphi_i \mid i \in \mathbb{N}\} \vdash \varphi \qquad \vdash \varphi_{i+1} \to \varphi_i \qquad \vdash \varphi \to \varphi_i \quad \forall i \in \mathbb{N}}{\{\neg M_{r+s}\varphi_i \mid i \in \mathbb{N}\} \vdash \neg M_r\varphi}, \quad s > 0$$

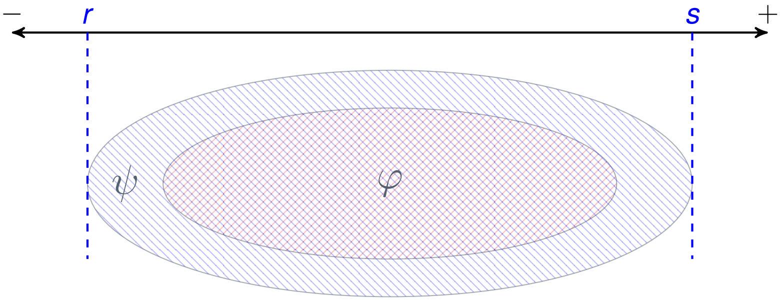
(R6): $\{L_{r+s}\varphi \mid \varphi \vdash F\} \cup \{\neg L_r\psi \mid F \vdash \psi\} \vdash \bot$

(R6′): $\{M_{r+s}\varphi \mid \varphi \vdash F\} \cup \{\neg M_r\psi \mid F \vdash \psi\} \vdash \bot$

Axioms
R2 and R2'

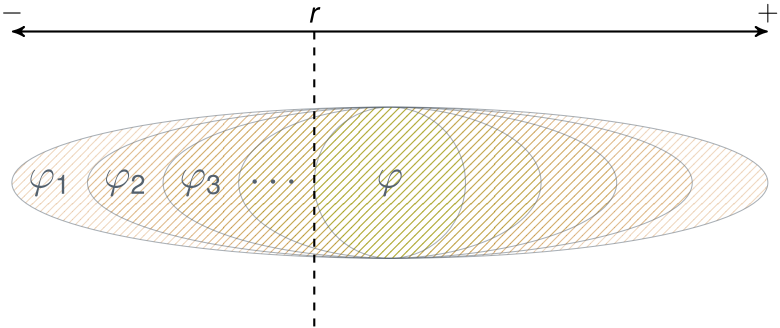
(R2) $\vdash \varphi \to \psi \implies ((L_r\psi) \wedge (L_0\varphi)) \to L_r\varphi$

(R2') $\vdash \varphi \to \psi \implies ((M_s\psi) \wedge (L_0\varphi)) \to M_s\varphi$



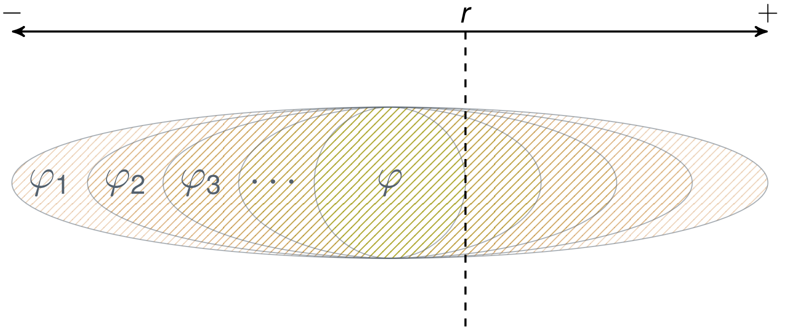
Axioms
R5

$$\textbf{(R5)} \quad \frac{\{\varphi_i \mid i \in \mathbb{N}\} \vdash \varphi \quad \vdash \varphi_{i+1} \to \varphi_i \quad \vdash \varphi \to \varphi_i \quad \forall i \in \mathbb{N}}{\{\neg L_r \varphi_i \mid i \in \mathbb{N}\} \vdash \neg L_{r+s}\varphi}, \quad s > 0$$



Axioms
R5'

$$\textbf{(R5')}\quad \frac{\{\varphi_i \mid i \in \mathbb{N}\} \vdash \varphi \quad \vdash \varphi_{i+1} \to \varphi_i \quad \vdash \varphi \to \varphi_i \quad \forall i \in \mathbb{N}}{\{\neg M_{r+s}\varphi_i \mid i \in \mathbb{N}\} \vdash \neg M_r \varphi}, \quad s > 0$$



Axioms
Soundness

Lemma (Soundness)

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

Canonical model construction

- GTS with ultrafilters as states.
- Transition function must satisfy conditions I-III.
  - $\theta_{\mathcal{L}} : \mathcal{U} \to [\mathcal{L} \to \mathcal{B}]$
  - $\theta_{\mathcal{F}} : \mathcal{U} \to [\mathcal{F} \cup \{\emptyset\} \to \mathcal{B}]$
  - $\theta_{\mathcal{U}} : \mathcal{U} \to [2^{\mathcal{U}} \to \mathcal{B}]$
- Labeling function $\ell_{\mathcal{U}} : \mathcal{U} \to 2^{\mathcal{AP}}$.
  - $\ell_{\mathcal{U}}(u) = \{p \in \mathcal{AP} \mid p \in u\}$

Formulae

Transition function to formulae

$$\theta_{\mathcal{L}}(u)(\varphi) = \begin{cases} \emptyset & \text{if } L_0\varphi \notin u \\ \langle \sup\{r \mid L_r\varphi \in u\}, \inf\{s \mid M_s\varphi \in u\}\rangle & \text{otherwise.} \end{cases}$$

The function $\theta_{\mathcal{L}}$ assigns a bound to each transition from an ultrafilter to a formula.

Lemma

$$L_0\varphi \in u \quad \text{implies} \quad \sup\{r \mid L_r\varphi \in u\} \leq \inf\{s \mid M_s\varphi \in u\}.$$

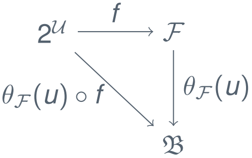
This means that the definition for $\theta_{\mathcal{L}}$ does not give ill-formed bounds.

Filters

Transition function to filters

$$\theta_{\mathcal{F}}(u)(F) = \biguplus_{\varphi \in [\![F]\!]} \theta_{\mathcal{L}}(u)(\varphi), \qquad [\![\Phi]\!] = \begin{cases} \{\bot\} & \text{if } \Phi = \emptyset \\ \{\varphi \in \mathcal{L} \mid \varphi \vdash \psi \text{ for all } \psi \in \Phi\} & \text{otherwise.} \end{cases}$$

Ultrafilters



f is an isomorphism between $2^{\mathcal{U}}$ and $\mathcal{F}$ given by

$$f(U) = \bigcap_{u \in U} u.$$

Ultrafilters

Transition function to sets of ultrafilters

$$\theta_{\mathcal{U}}(u)(U) = \theta_{\mathcal{F}}(u)(f(U)).$$

Theorem

The canonical model $\mathcal{G}_{\mathcal{U}} = (\mathcal{U}, \theta_{\mathcal{U}}, \ell_{\mathcal{U}})$ is a GTS.

Truth Lemma

Truth lemma

For consistent $\varphi \in \mathcal{L}$,

$$\mathcal{G}_{\mathcal{U}}, u \models \varphi \quad \text{iff} \quad \varphi \in u.$$

Weak completeness

Weak completeness

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

Proof

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

iff

$$\nvdash \varphi \quad \text{implies} \quad \not\models \varphi$$

iff

the consistency of $\neg\varphi$ implies the existences of a model for $\neg\varphi$

and this is true because of Lindenbaum's lemma and the truth lemma. □

Conclusion

Contribution

- New modelling formalism and logic with bounds to encode imprecisions.
  - Logic has the Hennessy-Milner property.
- Weak-complete axiomization.

Conclusion

Contribution

- New modelling formalism and logic with bounds to encode imprecisions.
  - Logic has the Hennessy-Milner property.
- Weak-complete axiomization.

Future work

- Strong completeness.
- Dependent axioms.
- Remove axioms with uncountably many instances.
- Relationship between WTS and GTS.

Thank you

Thank you!