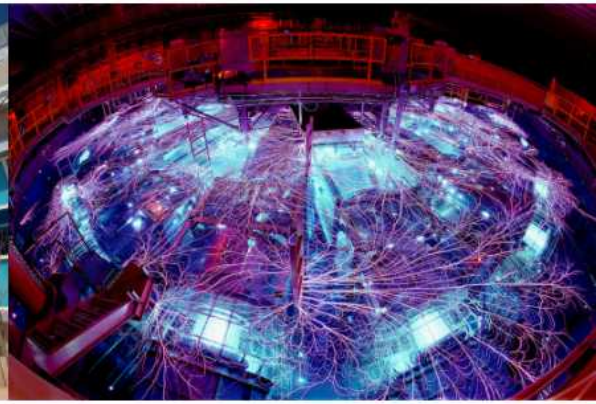
National Laboratories

SAND2019-8123C





A Topos Semantics for a Higher-order Temporal Logic of Actions

Philip Johnson-Freyd, **Jon Aytac**, Geoffrey C. Hulette

7/12/19

U.S. DEPARTMENT OF ENERGY

oratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia,
neywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract

Motivation

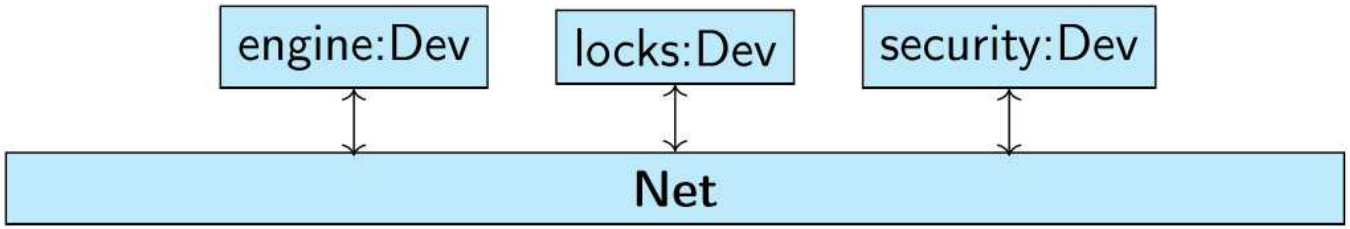
Motivation: Specifications of Temporal Behavior

Sandia National Laboratories

We want to build reactive systems from networks of devices

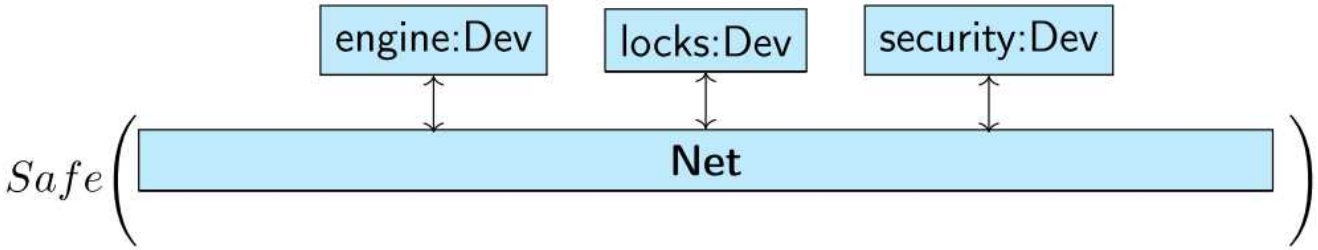
Motivation: Specifications of Temporal Behavior

We want to build reactive systems from networks of devices

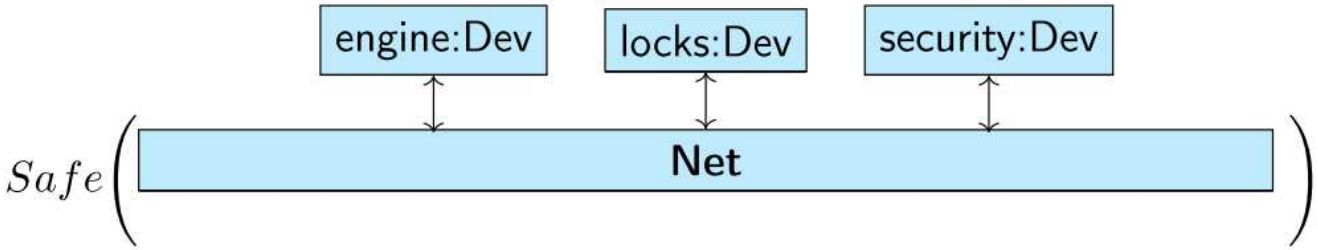


- For systems of high consequence, we should prove such a reactive system correct.

- For systems of high consequence, we should prove such a reactive system correct.

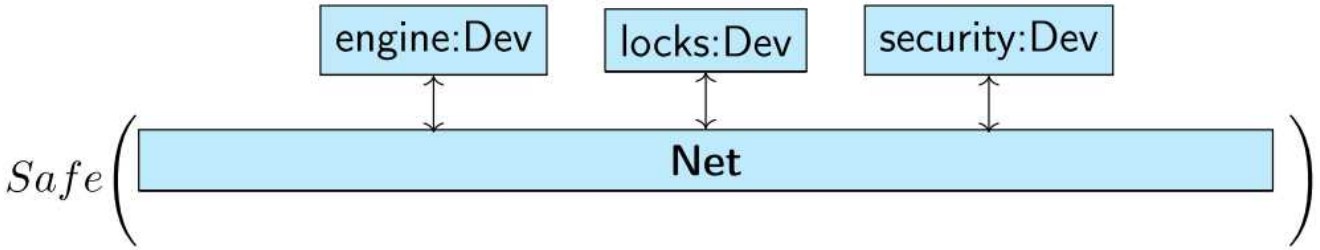


- For systems of high consequence, we should prove such a reactive system correct.



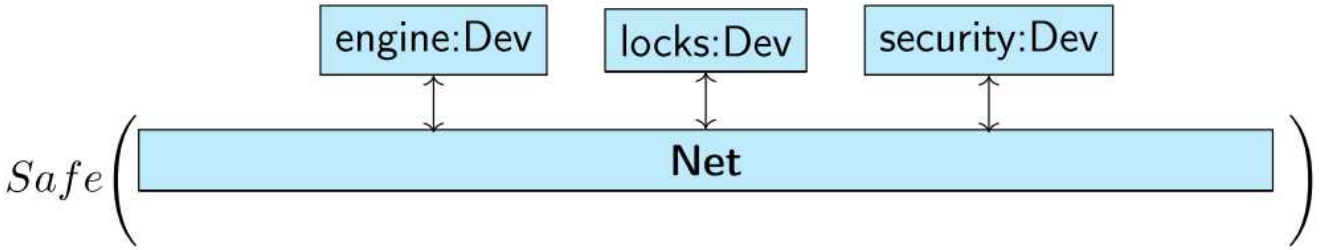
- As these systems are reactive, we must mean, by correctness, some specification of their allowed observable behaviors over the course of time

- For systems of high consequence, we should prove such a reactive system correct.



- As these systems are reactive, we must mean, by correctness, some specification of their allowed observable behaviors over the course of time
- Such properties are conveniently stated as formulae in temporal logic

- For systems of high consequence, we should prove such a reactive system correct.



- As these systems are reactive, we must mean, by correctness, some specification of their allowed observable behaviors over the course of time
- Such properties are conveniently stated as formulae in temporal logic
- The devices in the network are independently clocked, so our logic can't require synchrony.

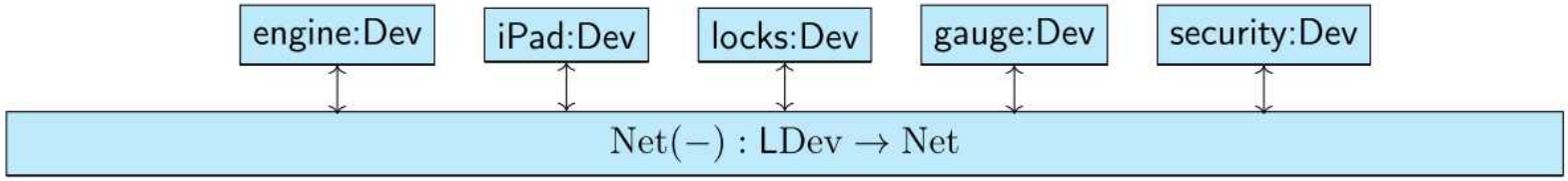
Motivation:Specifications of Temporal Behavior

Sandia National Laboratories

Actually, we don't know the list of devices ahead of time

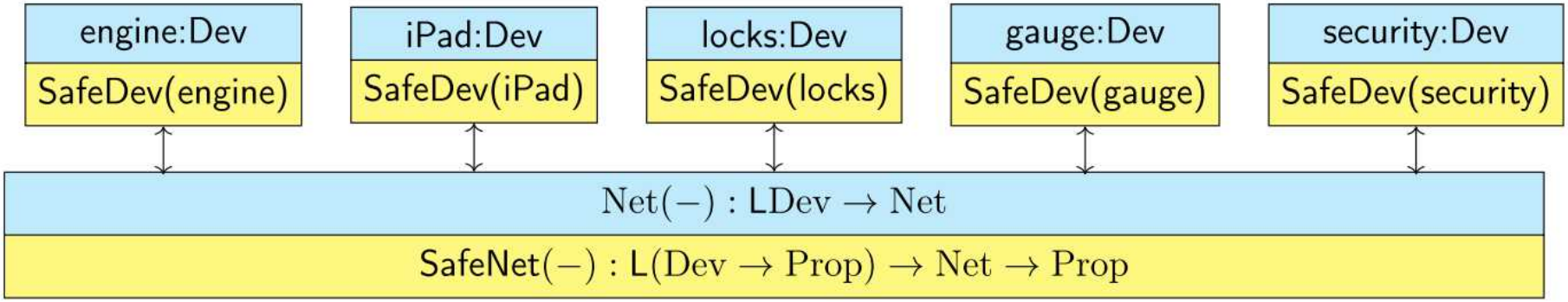
Motivation:Specifications of Temporal Behavior

Actually, we don't know the list of devices ahead of time



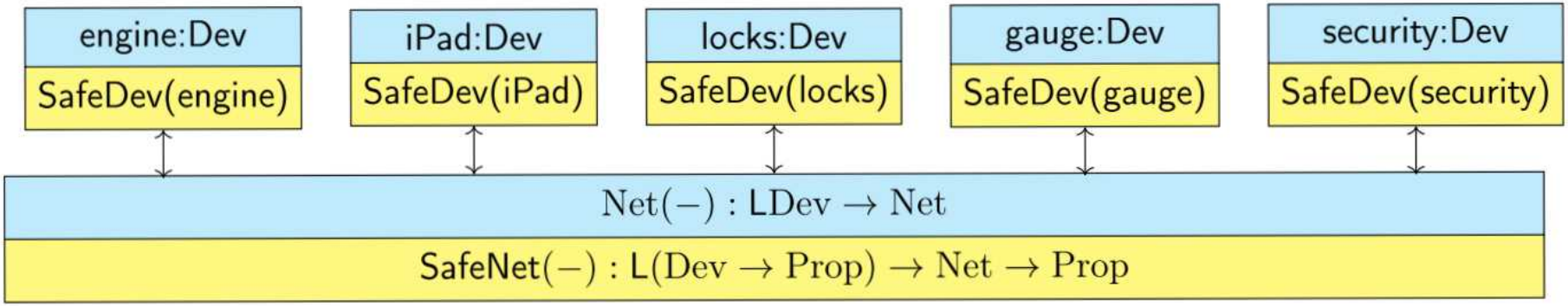
Motivation:Specifications of Temporal Behavior

So we actually need



Motivation:Specifications of Temporal Behavior

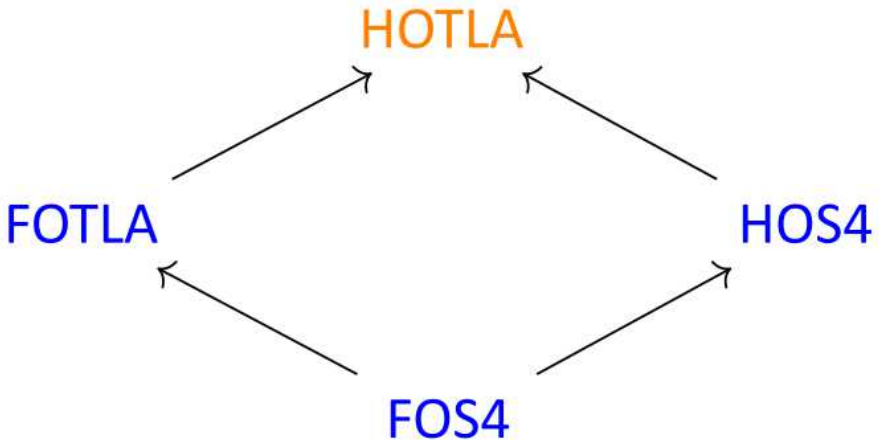
So we actually need



For this, we will need a higher-order temporal logic

Towards HOTLA

Our project is to try to unforget the top of this diagram



FOS4 = Temporal Logic
HOS4 = Higher-Order Logic
FOTLA = No Enforced Synchrony

Which Temporal Logic? Tense Logic?

Sandia National Laboratories

- Prior's tense logic

$$E \in \text{Expressions} := \mathbf{x} \mid x \mid f^n(E_1, \cdots, E_n)$$

$$T \in \text{Predicates} := P^n(E_1, \cdots, E_n) \mid T \wedge T \mid \exists x.T \mid \neg T \mid \Box T \mid \Diamond T$$

Which Temporal Logic? Tense Logic?

Sandia National Laboratories

- Prior's tense logic

$$E \in \text{Expressions} := \mathbf{x} \mid x \mid f^n(E_1, \cdots, E_n)$$
$$T \in \text{Predicates} := P^n(E_1, \cdots, E_n) \mid T \wedge T \mid \exists x.T \mid \neg T \mid \Box T \mid \Diamond T$$

- an S4 Modal logic (Kripke models over total orders).

Which Temporal Logic? Linear Temporal Logic?

- Pnuelli observed a shortcoming in Tense Logic- it has no way of describing instaneous changes

Which Temporal Logic? Linear Temporal Logic?

- Pnuelli observed a shortcoming in Tense Logic- it has no way of describing instaneous changes
- So he introduced an additional modality, $\circ$, to be thought of as "next". $T_1 \Rightarrow \circ T_2$ then means, having observed T_1 we will next observe T_2

Which Temporal Logic? Linear Temporal Logic?

- Pnuelli observed a shortcoming in Tense Logic- it has no way of describing instaneous changes
- So he introduced an additional modality, $\circ$, to be thought of as "next". $T_1 \Rightarrow \circ T_2$ then means, having observed T_1 we will next observe T_2
- This logic also has a well understood Kripke model (over $\mathbb{N}$). Unfortunately, the $\circ$ modality is fundamentally synchronous, and, so, inappropriate for our application.

The Temporal Logic of Actions

Sandia National Laboratories

- Recalling our example, the devices on our network are all independently clocked, so we can't capture the relevant examples with the ◦ modality

The Temporal Logic of Actions

Sandia National Laboratories

- Recalling our example, the devices on our network are all independently clocked, so we can't capture the relevant examples with the $\circ$ modality
- Lamport developed his Temporal Logic of Actions to solve this problem

Sandia National Laboratories

The (First-Order) Temporal Logic of Actions (FOTLA)

The (First Order) Temporal Logic of Actions

- As before, there are “rigid” variables (un-boldfaced) and “flexible” variables (boldfaced).

The (First Order) Temporal Logic of Actions

- As before, there are “rigid” variables (un-boldfaced) and “flexible” variables (boldfaced).
- As in Prior’s tense logic, one constructs from these the expressions and predicates

$$E \in \text{Terms} ::= x \mid \mathbf{x} \mid \mathbf{x}' \mid f(E_1, \ldots, E_n)$$

$$P \in \text{Propositions} ::= \Box P \mid \neg P \mid P_1 \wedge P_2 \mid \forall x.P \mid \Box[A]_{\langle \mathbf{x}_1, \cdots, \mathbf{x}_n \rangle}$$

The (First Order) Temporal Logic of Actions

- As before, there are “rigid” variables (un-boldfaced) and “flexible” variables (boldfaced).
- As in Prior’s tense logic, one constructs from these the expressions and predicates

$$E \in \text{Terms} ::= x \mid \mathbf{x} \mid \mathbf{x}' \mid f(E_1, \ldots, E_n)$$

$$P \in \text{Propositions} ::= \Box P \mid \neg P \mid P_1 \wedge P_2 \mid \forall x.P \mid \Box[A]_{\langle \mathbf{x}_1, \cdots, \mathbf{x}_n \rangle}$$

- To capture the idea of next, Actions, which classify changes

$$A \in \text{Actions} ::= R(E_1, \ldots, E_n) \mid E_1 = E_2 \mid \forall x.A \mid A_1 \wedge A_2 \mid \neg A$$

The Temporal Logic of *Actions*

- $\Box[A]_{\langle \mathbf{x}_1, \cdots, \mathbf{x}_n \rangle}$ always, the action predicate A is true or the flexible variables $\mathbf{x}_1, \cdots, \mathbf{x}_n$ remain unchanged

The Temporal Logic of *Actions*

- $\Box[A]_{\langle \mathbf{x}_1, \cdots, \mathbf{x}_n \rangle}$ always, the action predicate A is true or the flexible variables $\mathbf{x}_1, \cdots, \mathbf{x}_n$ remain unchanged
- This is the key feature which allows FOTLA to remedy tense logic's shortcomings without recourse to any notion of synchrony

Compositionality and the Syntax of the Temporal Logic of Actions

In order to express the proof obligation that one FOTLA specification be an abstraction of another, we need existential quantification over flexible variables

$$\textbf{Abstraction} \Rightarrow \exists \mathbf{x}.\textbf{Refinement}$$

The Syntax of the Temporal Logic of Actions

$$E \in \text{Terms} ::= x \mid \mathbf{x} \mid \mathbf{x}' \mid f(E_1, \ldots, E_n)$$

$$A \in \text{Actions} ::= R(E_1, \ldots, E_n) \mid E_1 = E_2 \mid \forall x.A \mid A_1 \wedge A_2 \mid \neg A$$

$$P \in \text{Propositions} ::= \Box P \mid \neg P \mid P_1 \wedge P_2 \mid \Box[A]_{<\mathbf{x}_1,\ldots,\mathbf{x}_n>} \mid \forall x.P \mid \forall \mathbf{x}.P$$

$$T \in \text{Formulae} ::= A \mid P$$

$$\exists x.T \triangleq \neg\forall x.\neg T$$

$$\exists \mathbf{x}.P \triangleq \neg\forall \mathbf{x}.\neg P$$

$$T_1 \vee T_2 \triangleq \neg(T_1 \wedge T_2) \quad T_1 \Rightarrow T_2$$

Discrete-Time Semantics for the First-Order Temporal Logic of Actions

The First-order Temporal Logic of Actions has a classical Discrete Time Semantics in Set.

Discrete-Time Semantics for the First-Order Temporal Logic of Actions

- Fix some set $\mathcal{D}$: Set modeling the domain of discourse

Discrete-Time Semantics for the First-Order Temporal Logic of Actions

- Fix some set $\mathcal{D}$: Set modeling the domain of discourse
- the *environment* θ : Rigid $\to \mathcal{D}$, the *state* σ : Flex $\to \mathcal{D}$, and the *next state* σ' : Flex' $\to \mathcal{D}$.

$\theta, \sigma, \sigma' \vDash A_1 \wedge A_2$	iff $(\theta, \sigma, \sigma' \vDash A_1)$ and $(\theta, \sigma, \sigma' \vDash A_1)$
$\theta, \sigma, \sigma' \vDash \neg A$	iff $\theta, \sigma, \sigma' \nvDash A$
$\theta, \sigma, \sigma' \vDash E_1 = E_2$	iff $[\![E_1]\!](\theta, \sigma, \sigma') = [\![E_2]\!](\theta, \sigma, \sigma')$
$\theta, \sigma, \sigma' \vDash \forall x.A$	iff for every $v \in \mathcal{D}$ $(\theta \uplus x \mapsto v), \sigma, \sigma' \vDash A$
$\theta, \sigma, \sigma' \vDash R(E_1, \ldots, E_n)$	iff $\mathcal{R}(R)([\![E_1]\!](\theta, \sigma, \sigma'), \ldots, [\![E_n]\!](\theta, \sigma, \sigma'))$

Discrete-Time Semantics for the FOTLA

- The interpretation of Predicates require, more than states, $\mathbb{N}$-indexed families of states called *behaviors*, $\rho = (\mathcal{D}^{\mathsf{Flex}})^{\mathbb{N}}$

Discrete-Time Semantics for the FOTLA

- The interpretation of Predicates require, more than states, $\mathbb{N}$-indexed families of states called *behaviors*, $\rho = (\mathcal{D}^{\text{Flex}})^{\mathbb{N}}$
- We can begin to give an interpretation of the FOTLA predicates

$\theta, \rho \models \Box P$ iff for every $n \in \mathbb{N}$ $\theta, \rho[n, ...] \models P$

$\theta, \rho \models \Box[A]_{<\mathbf{x_1},\ldots,\mathbf{x_m}>}$

iff for each $n \in \mathbb{N}$ either $\theta, \rho[n], \rho[n+1] \models A$

or $\forall i \in [1, m].\rho[n](\mathbf{x_i}) = \rho[n+1](\mathbf{x_i})$

$\theta, \rho \models \forall x.P$ iff for every $v \in \mathcal{D}$ $(\theta \uplus x \mapsto v), \rho \models P$

Discrete-Time Semantics for the FOTLA

But we can't give an interpretation for flexible quantification before defining an equivalence relation on behaviors.

Discrete-Time Semantics for the FOTLA

But we can't give an interpretation for flexible quantification before defining an equivalence relation on behaviors.

Definition (Discrete Stuttering Equivalence)

Let $(\mathcal{D}^{\mathsf{Flex}})^{\mathbb{N}}$ a collection of behaviors. Stuttering equivalence is the least equivalence relation on behaviors such that,
$\forall \rho \in (\mathcal{D}^{\mathsf{Flex}})^{\mathbb{N}}, n \in \mathbb{N}\ \rho' \simeq \rho$ when ρ' is given by

$$\rho'(m) = \rho(m) \text{ when } m \leq n \tag{2.1}$$

$$\rho'(m) = \rho(m-1) \text{ when } m > n \tag{2.2}$$

Discrete-Time Semantics for the FOTLA

Only now can we give flexible quantification an interpretation

$$\theta, \rho \vDash \forall \mathbf{x}.P$$

if and only if for every $d \in \mathcal{D}^{\mathbb{N}}$ and $\rho' \approx \rho, \theta, \rho' \uplus (\mathbf{x} \mapsto d) \vDash P$

Remark

to interpret quantification over flexible variables in the discrete time semantics, we must quantify over a stuttering equivalence class's worth of behaviors

Stuttering Invariance in the Discrete-Time Semantics for the FOTLA

Proposition (Stuttering Equivalence in FOTLA)

$\forall P, \theta, \rho, \rho'$ *such that* $\rho \simeq \rho'$

$$\theta, \rho \vDash P \textit{ if and only if } \theta, \rho' \vDash P$$

Continuous Time Semantics for the FOTLA

- The interpretation of rigid quantification was just quantification

Continuous Time Semantics for the FOTLA

- The interpretation of rigid quantification was just quantification
- The interpretation of flexible quantification required us to quantify over stuttering equivalent behaviors

Continuous Time Semantics for the FOTLA

Sandia National Laboratories

- The interpretation of rigid quantification was just quantification
- The interpretation of flexible quantification required us to quantify over stuttering equivalent behaviors
- A less ad hoc interpretation can be achieved in real time (Kaminsky and Yariv)

Continuous Time Semantics for the FOTLA

Sandia National Laboratories

- We take behaviors to be, rather than $\mathcal{D}^{\mathbb{N}}$, *some* sort of functions from $\mathbb{R}^{\geq 0}$ to the discrete set $\mathcal{D}$

Continuous Time Semantics for the FOTLA

Sandia National Laboratories

- We take behaviors to be, rather than $\mathcal{D}^{\mathbb{N}}$, *some* sort of functions from $\mathbb{R}^{\geq 0}$ to the discrete set $\mathcal{D}$
- What sort? Continuous?

Continuous Time Semantics for the FOTLA

Sandia National Laboratories

- We take behaviors to be, rather than $\mathcal{D}^{\mathbb{N}}$, *some* sort of functions from $\mathbb{R}^{\geq 0}$ to the discrete set $\mathcal{D}$
- What sort? Continuous?
- No, there aren't enough of those. At all.

Real-time Semantics for the FOTLA

Sandia National Laboratories

Definition (Non-Zeno function)

A non-Zeno function over a set S is a function f from non-negative real numbers to S such that

1. (Parmenedean) for every $t \in \mathbb{R}_{\geq 0}$ there exists a positive ϵ such that for all t' where $t \leq t' < t + \epsilon$ we have $f(t) = f(t')$ and
2. (Philiponean) there is no bounded increasing sequence $t_0, t_1, t_2, \ldots$ such that forall i, $f(t_i) \neq f(t_{i+1})$.

Continuous Time Semantics for the FOTLA

- Let us abuse the notation $\mathcal{D}^{\mathbb{R}_{\geq 0}}$ to refer to the set of non-Zeno functions over $\mathcal{D}$

Continuous Time Semantics for the FOTLA

- Let us abuse the notation $\mathcal{D}^{\mathbb{R}_{\geq 0}}$ to refer to the set of non-Zeno functions over $\mathcal{D}$
- Pre-composition by time-dilation gives an action $\mathrm{Hom}_{\mathsf{Top}}(\mathbb{R}_{\geq 0}, \mathbb{R}_{\geq 0}) \times \mathcal{D}^{\mathbb{R}_{\geq 0}} \to \mathcal{D}^{\mathbb{R}_{\geq 0}}$. relating stuttering equivalent behaviors.

Continuous Time Semantics for the FOTLA

- Let us abuse the notation $\mathcal{D}^{\mathbb{R}_{\geq 0}}$ to refer to the set of non-Zeno functions over $\mathcal{D}$
- Pre-composition by time-dilation gives an action $\mathsf{Hom}_{\mathsf{Top}}(\mathbb{R}_{\geq 0}, \mathbb{R}_{\geq 0}) \times \mathcal{D}^{\mathbb{R}_{\geq 0}} \to \mathcal{D}^{\mathbb{R}_{\geq 0}}$. relating stuttering equivalent behaviors.
- This allows a semantics where flexible and rigid quantification are just quantification over different sorts

Continuous Time Semantics for the FOTLA

$next(\tau, S) \triangleq 0$ when $\forall t \in \mathbb{R}_{\geq 0}, \forall x \in S, \tau(0)(x) = \tau(t)(x)$

$next(\tau, S) \triangleq \textbf{sup}\{r \mid \forall 0 \leq k \leq r, \forall x \in S, \tau(0)(x) = \tau(k)(x)\}$ otherwise

$\theta, \tau \models_{\mathbb{R}} \Box[A]_{\mathbf{x}_1,\ldots,\mathbf{x}_n}$ iff $r = 0$ or $\theta, \tau(0), \tau(r) \models A$

where $r = next(\tau, \{\mathbf{x}_i | 0 \leq i \leq n\})$

$\theta, \tau \models_{\mathbb{R}} \forall x.T$ iff for every $v \in \mathcal{D}$ we have $(\theta, x \mapsto v), \tau \models_{\mathbb{R}} T$

$\theta, \tau \models_{\mathbb{R}} \forall \mathbf{x}.T$ iff for every $v \in \mathcal{D}^{\mathbb{R}^+}$

we have $\theta, (x \mapsto (\tau(r), \mathbf{x} \mapsto v(r))) \models_{\mathbb{R}} T$

$\theta, \tau \models_{\mathbb{R}} \Box T$ iff for every $k \in \mathbb{R}_{\geq 0}$ such that $\theta, \tau[k..] \models_{\mathbb{R}} T$

Continuous Time Semantics for the FOTLA

- The uniform interpretation of quantification is suggestive of a multi-sorted first order language with categorical semantics interpreting the sorts Rigid and Flex as simply different objects in a category.

Continuous Time Semantics for the FOTLA

- The uniform interpretation of quantification is suggestive of a multi-sorted first order language with categorical semantics interpreting the sorts Rigid and Flex as simply different objects in a category.
- What we really want is higher-order.

Higer-Order Modal Logics (HOML)

Sandia National Laboratories

- We're interested in *higher-order modal* logics

Higer-Order Modal Logics (HOML)

Sandia National Laboratories

- We're interested in *higher-order modal* logics
- What are those? What are their categorical semantics?

Language of a HOML

- By higher-order logic, we mean a logic with the type and terms of the simply typed lambda calculus, a sort of Prop, and quantification over any type.
- The modal version adds a modality

$$\Box : \text{Prop} \rightarrow \text{Prop}$$

Algebraic Models of S4

Each fiber of our model will be a Heyting algebra, so, staring at the S4's wikipedia page , squinting to read $\vdash$ as $\preceq$, the axioms of S4 suggest an algebraic model

Definition

A **modal algebra** is a pair $(A, \Box) : \mathrm{Obj}(\mathrm{MAlg})$ where A is a Heyting algebra and $\Box$ is a left exact comonad on A.

A **modal algebra morphism** $f : (A, \Box) \to (B, \Box')$ is a morphism of the underlying Heyting algebras which commutes with the modalities in the sense that $f \cdot \Box = \Box' \cdot f$.

Models of HOS4

If we ask that our indexing category has enough stuff (cartesian closedness, a generic predicate) then we will be able to do the higher-order things

Models of HOL

Definition (Higher-order Hyperdoctrine)

A pair (C, P), where $\mathsf{P} : \mathsf{C}^{op} \to$ HeyAlg be a functor from a cartesion closed C into the category of Heyting algebras such that:

1. $\forall X, Y :$ ObjC there are *monotone* $\exists_Y^X, \forall_Y^X : \mathsf{P}(X \times Y) \to \mathsf{P}(Y)$ such that for $\pi : X \times Y \to Y$ the projection $\exists_Y^X \dashv \mathsf{P}(\pi) \dashv \forall_Y^X$ and satisfying the Beck-Chevalley condition $\forall f : Y \to Y'$

$$\begin{array}{ccc} \mathsf{P}(X \times Y') & \xrightarrow{\mathsf{P}(\mathrm{id}_X \times f)} & \mathsf{P}(X \times Y) \\ \forall_{Y'}^X \downarrow & & \downarrow \forall_Y^X \\ \mathsf{P}Y' & \xrightarrow[\mathsf{P}f]{} & \mathsf{P}Y \end{array}$$

   commutes as does the similar $\exists_Y^X$ diagram;

2. $(\mathsf{Forget} \cdot \mathsf{P}) : \mathsf{C}^{op} \to$ Set is representable.

Models of HOS4

Sandia National Laboratories

Definition (Modal Hyperdoctrine)

Let $\mathsf{P} : \mathsf{C}^{op} \to \mathsf{MAlg}$ be a functor from a small cartesian closed category C into the category of Modal algbras MAlg otherwise satisfying the axioms of a hyperdoctrine. Then (C, P) is a Modal Hyperdoctrine.

Higher-order Hyperdoctrines and Where to Find Them

Sandia National Laboratories

Fact

Let $\mathcal{T}$ be an elementary topos. Then $(\mathcal{T}, Hom_{\mathcal{T}}(-, \Omega))$ is a Higher-order Hyperdoctrine

Higher-order Hyperdoctrines and Where to Find Them

Sandia National Laboratories

Fact

Let $\mathcal{T}$ be an elementary topos. Then $(\mathcal{T}, Hom_{\mathcal{T}}(-, \Omega))$ is a Higher-order Hyperdoctrine

Fact

Let $\mathcal{E}$ be a topos, and H be a Heyting Algebra internal to $\mathcal{E}$. Then $(\mathcal{E}, Hom_{\mathcal{E}}(-, H))$ is a Higher-order Hyperdoctrine

Higher-order Modal Hyperdoctrines and Where to Find Them

Sandia National Laboratories

Definition

Let $\mathcal{E}$, $\mathcal{F}$ be topoi. A **geometric morphism** f : $\mathcal{E} \to \mathcal{F}$ is an adjunction

$$\mathcal{E} \underset{\mathsf{f}^\star}{\overset{\mathsf{f}_\star}{\underset{\longleftarrow}{\overset{\longrightarrow}{\top}}}} \mathcal{F}$$

such that the left adjoint $\mathsf{f}^\star$, known as the inverse image, preserves finite limits. If every object $X : \mathrm{Obj}(\mathcal{E})$ is a subquotient of an object of the inverse image $\mathsf{f}^\star$, so that there exists $Y : \mathrm{Obj}(\mathcal{F})$ and diagram $f^\star(Y) \leftarrowtail S \twoheadrightarrow X$, then f is **localic**.

Higher-order Modal Hyperdoctrines and Where to Find Them

Sandia National Laboratories

Proposition

Let $\mathsf{f} : \mathcal{E} \to \mathcal{F}$ *a geometric morphism. Then* $\mathsf{f}_\star(\Omega_\mathcal{E})$ *is a complete Heyting algebra internal to* $\mathcal{F}$*.*

Sandia National Laboratories

Lemma (johnstone, sketches C1.3)

In any topos $\mathcal{E}$, the subobject classifier $\Omega_{\mathcal{E}}$ is the initial complete Heyting algebra object. That is, for all complete Heyting algebras H internal to $\mathcal{E}$, there is a unique map of complete Heyting algebras $i : \Omega_{\mathcal{E}} \to H$. Moreover, the right adjoint of τ is the classifying map of the top element $\top_H : 1 \to H$.

Higher-order Modal Hyperdoctrines and Where to Find Them

Sandia National Laboratories

Lemma (Awodey, Kishida, Kotzsch)

Given a complete Heyting algebra H internal to topos $\mathcal{E}$, let $i \vdash \tau$ the canonical adjunction $i : \Omega_{\mathcal{E}} \overset{\rightarrow}{\leftarrow} H : \tau$. The composite $i \circ \tau$ is an S4 modality on H.

Higher-order Modal Hyperdoctrines and Where to Find Them

Sandia National Laboratories

Example

Let K be a preorder, interpreted as a collection of "possible worlds," together with an accessibility relation. By $|K|$ we mean the discrete category with the same underlying objects as K. The inclusion $|K| \to K$ induces a geometric morphism f : $Psh(|K|) \to Psh(K)$.

Higher-order Modal Hyperdoctrines and Where to Find Them

Sandia National Laboratories

Example

Let K be a preorder, interpreted as a collection of "possible worlds," together with an accessibility relation. By $|K|$ we mean the discrete category with the same underlying objects as K. The inclusion $|K| \to K$ induces a geometric morphism $\mathsf{f} : Psh(|K|) \to Psh(K)$.

Lemma (johnstone, 1981, prop. 3.1)

Let $\mathsf{f} : \mathsf{D} \to \mathsf{C}$ *be a functor of small categories. If* f *is faithful, then the induced geometric morphism* $Psh(\mathsf{D}) \to Psh(\mathsf{C})$ *is localic.*

Sandia National Laboratories

Continuous-Time Semantics, Categorically

A Model for HOTLA

Sandia National Laboratories

Definition (Stutter)

A stutter is a continuous function $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ with continuous inverse.

By $\mathcal{S}$ we denote the group of stutters

$$\mathcal{S} = (\{f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} \mid f \text{ is a stutter}\}, \cdot, id_{\mathbb{R}_{\geq 0}})$$

.

A Model for HOTLA

Sandia National Laboratories

Definition (Stutter)

A stutter is a continuous function $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ with continuous inverse.

By $\mathcal{S}$ we denote the group of stutters

$$\mathcal{S} = (\{f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} \mid f \text{ is a stutter}\}, \cdot, id_{\mathbb{R}_{\geq 0}})$$

.

Remark

continuous semantics, stuttering invariance is precisely closure under the action the group of stutters.

A Model for HOTLA

Sandia National Laboratories

Definition (Stutter)

A stutter is a continuous function $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ with continuous inverse.

By $\mathcal{S}$ we denote the group of stutters

$$\mathcal{S} = (\{f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} \mid f \text{ is a stutter}\}, \cdot, id_{\mathbb{R}_{\geq 0}})$$

.

Remark

continuous semantics, stuttering invariance is precisely closure under the action the group of stutters.

Remark

Fixing a domain of discourse, the collection of all stuttering invariant behaviors is an $\mathcal{S}$-set, and stuttering invariant sub-sets are $\mathcal{S}$-subsets.

A Model for HOTLA

This suggests interpreting HOTLA's sorts as objects in $\mathrm{Psh}(\mathrm{B}\mathcal{S})$. Are these our temporal types?

A Model for HOTLA

This suggests interpreting HOTLA's sorts as objects in $\mathrm{Psh}(\mathrm{B}\mathcal{S})$. Are these our temporal types?

Remark

A behavior (viewed as a non-Zeno function) is always a member of some set of behaviors if, given any initial delay in which the behavior is not observed, the remainder is in that set.

A Model for HOTLA

This suggests interpreting HOTLA's sorts as objects in $\mathrm{Psh}(\mathrm{B}\mathcal{S})$. Are these our temporal types?

Remark

A behavior (viewed as a non-Zeno function) is always a member of some set of behaviors if, given any initial delay in which the behavior is not observed, the remainder is in that set.

Thus, while stuttering invariance has to do with closure under dilation of time by bi-continuous functions, $\Box$ has to do with the translation of time.

A Model for HOTLA

Sandia National Laboratories

Definition

A falter is a monotone function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ such that the function $x \mapsto f(x) - f(0)$ is a stutter.

By $\mathcal{F}$ we denote the monoid of falters (under function composition).

A Model for HOTLA

Sandia National Laboratories

Remark

The inclusion $\iota : \mathcal{S} \to \mathcal{F}$ induces a faithful functor $\iota : \mathsf{B}\mathcal{S} \to \mathsf{B}\mathcal{F}$. Such a faithful functor induces a localic geometric morphism on the associated presheaf categories $\iota^\star \dashv \iota_\star : Psh(\mathsf{B}\mathcal{S}) \overset{\to}{\leftarrow} Psh(\mathsf{B}\mathcal{F})$.

A Model for HOTLA

So our temporal types are objects in $Psh(\mathsf{B}\mathcal{F})$

A Model for HOTLA

Sandia National Laboratories

So our temporal types are objects in $Psh(\mathsf{B}\mathcal{F})$

$$\mathsf{Flex} : \mathsf{Set} \to Psh(\mathsf{B}\mathcal{F})$$

$$\mathsf{Flex}(\mathcal{D}) = (\{f : \mathbb{R}_{\geq 0} \to \mathcal{D} \mid f \text{ non zeno}\}, \cdot)$$

A Model for HOTLA

So our temporal types are objects in $Psh(\mathsf{B}\mathcal{F})$

$$\mathsf{Flex} : \mathsf{Set} \to Psh(\mathsf{B}\mathcal{F})$$
$$\mathsf{Flex}(\mathcal{D}) = (\{f : \mathbb{R}_{\geq 0} \to \mathcal{D} \mid f \text{ non zeno}\}, \cdot)$$

$$\mathsf{Rigid} : \mathsf{Set} \to Psh(\mathsf{B}\mathcal{F})$$
$$\mathsf{Rigid}(\mathcal{D}) = (\mathcal{D}, ((\_, x) \mapsto x))$$

A Model for HOTLA

- As $\mathcal{S}$ is a group, it has only two ideals, $\emptyset$ and $\mathcal{S}$. Thus, $\Omega_{Psh(\mathsf{B}\mathcal{S})}$ is the set 2 with the trivial $\mathcal{S}$-action. So $\iota_\star\Omega_{Psh(\mathsf{B}\mathcal{S})}$ is a complete *Boolean* algebra internal to $Psh(\mathsf{B}\mathcal{F})$

A Model for HOTLA

Sandia National Laboratories

- As $\mathcal{S}$ is a group, it has only two ideals, $\emptyset$ and $\mathcal{S}$. Thus, $\Omega_{Psh(\mathsf{B}\mathcal{S})}$ is the set 2 with the trivial $\mathcal{S}$-action. So $\iota_\star \Omega_{Psh(\mathsf{B}\mathcal{S})}$ is a complete *Boolean* algebra internal to $Psh(\mathsf{B}\mathcal{F})$
- As the geometric morphism $\iota^\star \dashv \iota_\star : Psh(\mathsf{B}\mathcal{S}) \overset{\rightarrow}{\leftarrow} Psh(\mathsf{B}\mathcal{F})$ is localic, we should be able to compute a non-trivial modality.

A Model for HOTLA

- As presheaf categories have all (co)limits, the inverse image part of the geometric morphism may be computed as a right Kan extension.

A Model for HOTLA

- As presheaf categories have all (co)limits, the inverse image part of the geometric morphism may be computed as a right Kan extension.
- B$\mathcal{S}$ and B$\mathcal{F}$ have singleton objects, so we can compute pointwise

A Model for HOTLA

- As presheaf categories have all (co)limits, the inverse image part of the geometric morphism may be computed as a right Kan extension.
- $\mathsf{B}\mathcal{S}$ and $\mathsf{B}\mathcal{F}$ have singleton objects, so we can compute pointwise
- Given $\mathsf{F} : \mathsf{Set}^{\mathsf{B}\mathcal{S}}$, we compute $\lim \left(\bullet_{\mathcal{S}} \downarrow \iota \xrightarrow{\pi^{\bullet_{\mathcal{S}}}} \mathsf{B}\mathcal{S} \xrightarrow{\mathsf{F}} \mathsf{Set} \right)$

A Model for HOTLA

this amounts to equalizing away the stutter action

$$\prod_{\mathcal{S}\setminus\mathcal{F}} \mathsf{F}(\bullet_{\mathcal{S}}) \rightarrowtail \prod_{\mathcal{F}} \mathsf{F}(\bullet_{\mathcal{S}}) \rightrightarrows \prod_{\mathcal{S}\times\mathcal{F}} \mathsf{F}(\bullet_{\mathcal{S}}) \ .$$

A Model for HOTLA

On $Psh(\mathsf{B}\mathcal{S})$'s subobject classifier, this is

$$\begin{aligned}\mathsf{Prop} &\triangleq \iota_\star(\Omega_{Psh(\mathsf{B}\mathcal{S})}) \\ &= (\{p : \mathcal{F} \to 2 \mid \forall m \in \mathcal{S}, n \in \mathcal{F}, p(n) = p(nm)\} \\ &\qquad , \quad (n, p) \mapsto (r' \mapsto p(n \cdot n'))) \\ &\cong (\mathcal{P}(\mathbb{R}_{\geq 0}), (n, O) \mapsto \mathsf{im}^{-1}(n)(O))\end{aligned}$$

A Model for HOTLA

On $Psh(\mathsf{B}\mathcal{S})$'s subobject classifier, this is

$$\begin{aligned}\mathsf{Prop} &\triangleq \iota_\star(\Omega_{Psh(\mathsf{B}\mathcal{S})}) \\ &= (\{p : \mathcal{F} \to 2 \mid \forall m \in \mathcal{S}, n \in \mathcal{F}, p(n) = p(nm)\} \\ &\qquad , \quad (n, p) \mapsto (r' \mapsto p(n \cdot n'))) \\ &\cong (\mathcal{P}(\mathbb{R}_{\geq 0}), (n, O) \mapsto \mathsf{im}^{-1}(n)(O))\end{aligned}$$

Consequently (and pleasingly), in our model, a proposition corresponds to the set of times when that proposition is true.

A Model for HOTLA

- The subobject classifier in $Psh(\mathsf{B}\mathcal{F})$ is the collection of falter ideals

$$\Omega_{Psh(\mathsf{B}\mathcal{F})} = \{I \subseteq \mathcal{F} \mid \forall i \in I \, \forall f \in \mathcal{F} \,.\, i \cdot f \in I\},$$

A Model for HOTLA

- The subobject classifier in $Psh(\mathsf{B}\mathcal{F})$ is the collection of falter ideals

$$\Omega_{Psh(\mathsf{B}\mathcal{F})} = \{I \subseteq \mathcal{F} \mid \forall i \in I \, \forall f \in \mathcal{F} \,.\, i \cdot f \in I\},$$

- but these are just all upward-closed subsets of $\mathbb{R}_{\geq 0}$, so $\Omega_{Psh(\mathsf{B}\mathcal{F})} \cong \langle \mathcal{P}_{\uparrow}(\mathbb{R}_{\geq 0}), (n, O) \mapsto \mathsf{im}^{-1}(n)(O) \rangle$.

A Model for HOTLA

- As subobject classifier in $Psh(\mathsf{B}\mathcal{F})$, $\Omega_{Psh(\mathsf{B}\mathcal{F})}$ is initial in complete Heyting algebras internal to $\mathcal{F}$

A Model for HOTLA

- As subobject classifier in $Psh(\mathsf{B}\mathcal{F})$, $\Omega_{Psh(\mathsf{B}\mathcal{F})}$ is initial in complete Heyting algebras internal to $\mathcal{F}$
- so the obvious equivariant inclusion $i_\Omega : \Omega_{Psh(\mathsf{B}\mathcal{F})} \hookrightarrow \iota_\star(\Omega_{Psh(\mathsf{B}\mathcal{S})})$ is essentially unique.

A Model for HOTLA

- As subobject classifier in $Psh(\mathsf{B}\mathcal{F})$, $\Omega_{Psh(\mathsf{B}\mathcal{F})}$ is initial in complete Heyting algebras internal to $\mathcal{F}$
- so the obvious equivariant inclusion $i_\Omega : \Omega_{Psh(\mathsf{B}\mathcal{F})} \hookrightarrow \iota_\star(\Omega_{Psh(\mathsf{B}\mathcal{S})})$ is essentially unique.
- The right adjoint is the τ_Ω is a pullback. which is, then, the upward closure $\uparrow(-) : \mathcal{P}(\mathbb{R}) \to \mathcal{P}_\uparrow(\mathbb{R})$.

A Model for HOTLA

- The adjunction $\Box := i_\Omega \circ \tau_\Omega : \mathsf{End}(\iota_\star \Omega_{Psh(\mathsf{B}\mathcal{S})})$ provides a left exact comonad on the complete internal Heyting algebra $\iota_\star(\Omega_{Psh(\mathsf{B}\mathcal{S})})$.

A Model for HOTLA

- The adjunction $\Box := i_\Omega \circ \tau_\Omega : \mathsf{End}(\iota_\star \Omega_{Psh(\mathsf{B}\mathcal{S})})$ provides a left exact comonad on the complete internal Heyting algebra $\iota_\star(\Omega_{Psh(\mathsf{B}\mathcal{S})})$.
- The resulting modal structure is quite natural – it reduces to ensuring that a proposition holds at all future times

$$\Box(-) : \mathsf{Prop} \to_{Psh(\mathsf{B}\mathcal{F})} \mathsf{Prop}$$
$$\Box(S) = \{r \in \mathbb{R}_{\geq 0} \mid \forall r' \geq r, r' \in S\}.$$

A Model for HOTLA

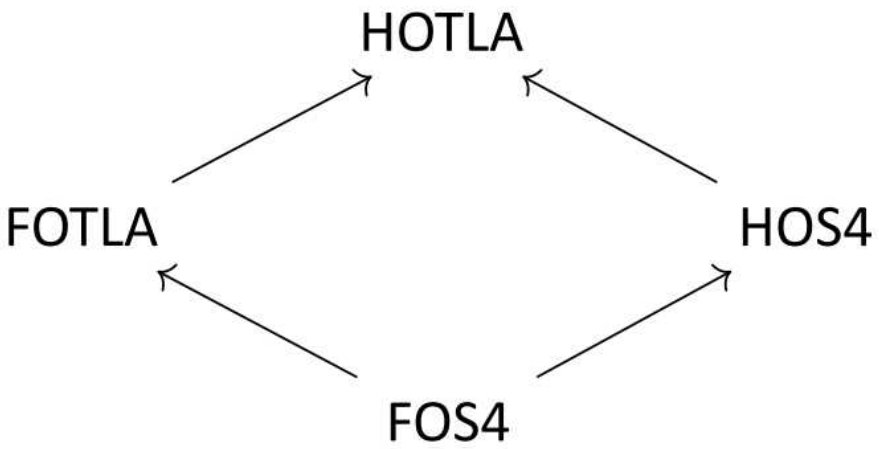
Sandia National Laboratories

Theorem

The modal hyperdoctrine $(Psh(\mathsf{B}\mathcal{F}), Hom(-, \iota_\star(\Omega_{\mathsf{B}\mathcal{S}})))$ *admits a sound interpretation of higher-order classical S4. Moreover, restricting to the first-order fragment corresponds to the existing semantics of TLA.*

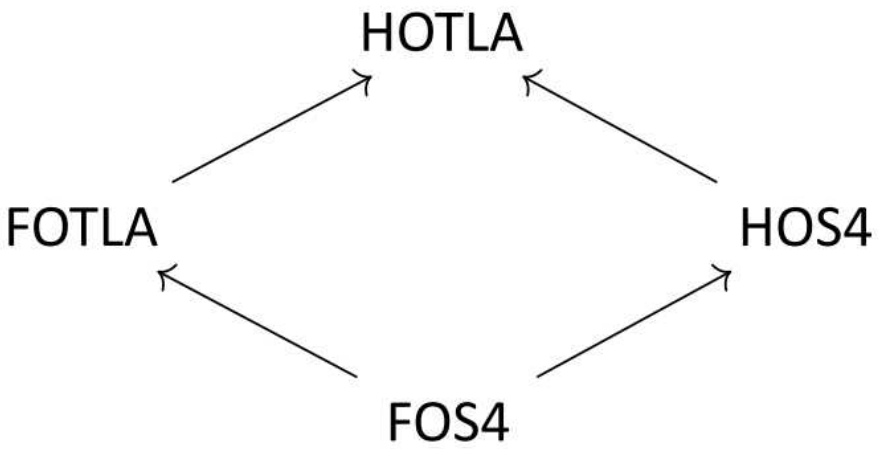
Towards HOTLA

In a sense, our project is to try to unforget the top of this diagram



Towards HOTLA

In a sense, our project is to try to unforget the top of this diagram



As a first step, inspired by the Continuous Time semantics of FOTLA, we've begun to sketch, in this work, what will surely prove to be HOTLA's model once someone gets around to writing down HOTLA's syntax.

Bonus Slides

Sandia National Laboratories

Bonus Slides

Outlook

- There is an equivalence $\mathrm{Log}_{\tau}(\mathcal{E}_{\mathbb{T}}, (\mathcal{E}, H)) \simeq \mathrm{Mod}_{\mathbb{T}}(\mathcal{E}, H)$ between a suitable category of logical functors from the syntactic category of a theory into and models of the theory in the modal hyperdoctrine $(\mathcal{E}, H)$. So, given a candidate syntax for HOTLA, we should be able to test for the existence of such a functor into our model.

Outlook

- There is an equivalence $\mathrm{Log}_{\tau}(\mathcal{E}_{\mathbb{T}}, (\mathcal{E}, H)) \simeq \mathrm{Mod}_{\mathbb{T}}(\mathcal{E}, H)$ between a suitable category of logical functors from the syntactic category of a theory into and models of the theory in the modal hyperdoctrine $(\mathcal{E}, H)$. So, given a candidate syntax for HOTLA, we should be able to test for the existence of such a functor into our model.
- Model in hand, we can, given a syntax for HOTLA, check the validity of proposed proof rules

Outlook

- There is an equivalence $\mathrm{Log}_{\tau}(\mathcal{E}_{\mathbb{T}}, (\mathcal{E}, H)) \simeq \mathrm{Mod}_{\mathbb{T}}(\mathcal{E}, H)$ between a suitable category of logical functors from the syntactic category of a theory into and models of the theory in the modal hyperdoctrine $(\mathcal{E}, H)$. So, given a candidate syntax for HOTLA, we should be able to test for the existence of such a functor into our model.
- Model in hand, we can, given a syntax for HOTLA, check the validity of proposed proof rules
- Topoi have all finite limits, so we should be able to form compositions over shared interfaces via pullback

On Compositionality

Sandia National Laboratories

Composition: A Way to Make Proofs Harder

Leslie Lamport

24 December 1997

Appeared in *Compositionality: The Significant Difference (Proceedings of the COMPOS'97 Symposium)*, Willem-Paul de Roever, Hans Langmaack, and Amir Pnueli editors. Lecture Notes in Computer Science, number 1536, (1998), 402–423.

Higher-order Modal Hyperdoctrines and Where to Find Them

Thus we obtain a modal hyperdoctrine on $(Psh(K), \mathsf{Hom}_{Psh(K)}(-, \mathsf{f}_\star(\Omega_{Psh(|K|)})))$. In particular, as $|K|$ is a groupoid, $\mathcal{E} = Psh(|K|)$ is a Boolean topos, so $\mathsf{f}_\star(\Omega_\mathcal{E})$ is not only a complete Heyting algebra internal to $\mathcal{F} = Psh(K)$, it is an internal Boolean algebra! The resulting logic is classical, even though $Psh(K)$ is very much not a boolean topos in general (it is, instead, a Kripke model of an intuitionistic logic). The

Deductive System on Type Prop in a HOML Language

- A relation $\vdash$ between terms of type Prop characterized by the rules of intuitionist higher-order logic with two new rules for the modality
- modal function extensionality

$$\frac{f, g : S \to T}{\Box \forall x : A. f(x) =_T g(x) \vdash f =_{S \to T} g}$$

- modal propositional extensionality $\dfrac{p, q : \mathsf{Prop}}{\Box(p \Leftrightarrow q) \vdash p =_{\mathsf{Prop}} q}$

Higher-order Modal Theories (HOMT)

Sandia National Laboratories

Definition

A theory in a HOML Language is a collection of axioms of the form $\Gamma \vdash \top \vdash \alpha$, where Γ are contexts and α are terms, in the empty context, well-typed of type Prop

Categorical Semantics of Multi-Sorted First-Order Logic

Definition (First-Order Hyperdoctrine Cont'd)

(equality) For all $\Delta_X = \langle 1_X, 1_X \rangle : X \to X \times X$, $\mathsf{P}(\Delta_X)$ has a left adjoint satisfying the Beck-Chevalley condition

$$\begin{array}{ccc} X & \xrightarrow{\Delta_X} & X \times X \\ {\scriptstyle \Delta_X}\downarrow & & \downarrow{\scriptstyle 1 \times \Delta_X} \\ X \times X & \xrightarrow[\Delta_X \times 1_X]{} & X \times X \times X \end{array}$$

and (generic predicate)

$(\text{Forget} \circ \mathsf{P}) : \mathsf{C}^{op} \to \text{Set}$. Then (C, P) is a **First-Order Hyperdoctrine**

S4 Theories

Recall, any S4 Theory (be it HOS4 or FOS4) must include the axioms

- $$\frac{\Gamma \mid \varphi \vdash \psi}{\Gamma \mid \Box\varphi \vdash \Box\psi}$$
- $$\frac{}{\Gamma \mid \top \vdash \Box\top}$$
- $$\frac{}{\Gamma \mid \Box\varphi \wedge \Box\psi \vdash \Box(\varphi \wedge \psi)}$$
- $$\frac{}{\Gamma \mid \Box\varphi \vdash \varphi}$$
- $$\frac{}{\Gamma \mid \Box\varphi \vdash \Box\Box\varphi}$$