A topos-theoretic approach to systems and behavior

David I. Spivak* and Patrick Schultz

Mathematics Department
Massachusetts Institute of Technology

Toposes in Como
June 27, 2018
Outline

1 Introduction
   - The National Airspace System
   - Summary: motivation and plan

2 The topos $B$ of behavior types

3 Temporal type theory

4 Application to the NAS

5 Conclusion

An example system

The National Airspace System (NAS)

- Goals of NextGen:
  - Double the number of airplanes in the sky;
  - Remain extremely safe.

1 Traffic Collision Avoidance System.
The National Airspace System (NAS)

- **Goals of NextGen:**
  - Double the number of airplanes in the sky;
  - Remain extremely safe.
- **Safe separation problem:**
  - Planes need to remain at a safe distance.
  - Can’t generally communicate directly.
  - Use radars, pilots, ground control, radios, and TCAS.¹

¹Traffic Collision Avoidance System.
**An example system**

The National Airspace System (NAS)
- **Goals of NextGen:**
  - Double the number of airplanes in the sky;
  - Remain extremely safe.
- **Safe separation problem:**
  - Planes need to remain at a safe distance.
  - Can’t generally communicate directly.
  - Use radars, pilots, ground control, radios, and TCAS.\(^1\)
- **Systems of systems:**
  - A great variety of interconnected systems.
  - Work in concert to enforce global property: safe separation.

---

\(^1\) Traffic Collision Avoidance System.
Systems of interacting systems in the NAS
Systems of interacting systems in the NAS
Behaviors as sheaves, “contracts” as predicates

Everything in sight will be assigned a sheaf.
- A sheaf of possible behaviors for each box.
- A sheaf of possible behaviors (signals) for each wire.
- Sheaf morphisms from boxes to their wires.
Behaviors as sheaves, “contracts” as predicates

- Everything in sight will be assigned a sheaf.
  - A sheaf of possible behaviors for each box.
  - A sheaf of possible behaviors (signals) for each wire.
  - Sheaf morphisms from boxes to their wires.

- A plane behavior has an associated altitude behavior, TCAS behavior, etc.
  - Want to write it all logically and prove global property.
  - Ask boxes to satisfy predicates = “contracts” = relations on their wires.
  - If everyone satisfies their contract, system maintains safe separation.
What’s the topos for the National Airspace System?
- This question was a major guide for our work.
- Need to combine many common frameworks into a “big tent”.
  - Differential equations, continuous dynamical systems.
  - Labeled transition systems, discrete dynamical systems.
  - Delays, non-instantaneous rules.
  - Determinism, non-determinism.
NAS use-case as guide

What’s the topos for the National Airspace System?
- This question was a major guide for our work.
- Need to combine many common frameworks into a “big tent”.
  - Differential equations, continuous dynamical systems.
  - Labeled transition systems, discrete dynamical systems.
  - Delays, non-instantaneous rules.
  - Determinism, non-determinism.
- Need a logic in which to prove safety of the combined system.
  - Currently, combination process takes place in engineers’ heads.
  - For NextGen, we may need to do better.
NAS use-case as guide

What’s the topos for the National Airspace System?
- This question was a major guide for our work.
- Need to combine many common frameworks into a “big tent”.
  - Differential equations, continuous dynamical systems.
  - Labeled transition systems, discrete dynamical systems.
  - Delays, non-instantaneous rules.
  - Determinism, non-determinism.
- Need a logic in which to prove safety of the combined system.
  - Currently, combination process takes place in engineers’ heads.
  - For NextGen, we may need to do better.

Relationship to toposes:
- Toposes have an associated internal language and logic.
- Can use formal methods (proof assistants) to prove properties of NAS.
Plan of the talk

1. Define a topos $\mathcal{B}$ of behavior types.

2. Discuss *temporal type theory*, which is sound in $\mathcal{B}$.

3. Return to our NAS use-case.
Outline

1. Introduction

2. The topos $\mathcal{B}$ of behavior types
   - Choosing a topos
   - An intervallic time-line, $\mathbb{IR}$
   - $\mathcal{B}$ the topos of behavior types

3. Temporal type theory

4. Application to the NAS

5. Conclusion

What is behavior?

We want to model behavior.

- What behaves in this sense?
What is behavior?

We want to model behavior.

- What behaves in this sense?
  - You, your thoughts, your body, your airplane.
  - The radio, each movie, each fight, each fighter.
  - Any sort of thing that can “happen”.
What is behavior?

We want to model behavior.

- What behaves in this sense?
  - You, your thoughts, your body, your airplane.
  - The radio, each movie, each fight, each fighter.
  - Any sort of thing that can “happen”.

- What is a behavior type?
  - A behavior type is like “airplane behavior” or “pilot behavior”
  - Both are collections of possibilities, indexed by time intervals.
  - I want to conceptualize them as sheaves on time intervals.
What is behavior?

We want to model behavior.

- What behaves in this sense?
  - You, your thoughts, your body, your airplane.
  - The radio, each movie, each fight, each fighter.
  - Any sort of thing that can “happen”.

- What is a behavior type?
  - A behavior type is like “airplane behavior” or “pilot behavior”
  - Both are collections of possibilities, indexed by time intervals.
  - I want to conceptualize them as sheaves on time intervals.

So what should we mean by time?
What is behavior?

We want to model behavior.

- What behaves in this sense?
  - You, your thoughts, your body, your airplane.
  - The radio, each movie, each fight, each fighter.
  - Any sort of thing that can “happen”.

- What is a behavior type?
  - A behavior type is like “airplane behavior” or “pilot behavior”
  - Both are collections of possibilities, indexed by time intervals.
  - I want to conceptualize them as sheaves on time intervals.

So what should we mean by time?

- Only rule: whatever we mean, we should be able to capture:
  - Differential equations, labeled transition systems, delay...
What is behavior?

We want to model behavior.

- What behaves in this sense?
  - You, your thoughts, your body, your airplane.
  - The radio, each movie, each fight, each fighter.
  - Any sort of thing that can “happen”.

- What is a behavior type?
  - A behavior type is like “airplane behavior” or “pilot behavior”
  - Both are collections of possibilities, indexed by time intervals.
  - I want to conceptualize them as sheaves on time intervals.

So what should we mean by time?

- Only rule: whatever we mean, we should be able to capture:
  - Differential equations, labeled transition systems, delay...
  - ...compositionally: prove properties of combined systems.
First guess: \( \mathbb{R} \) as timeline

\( \mathbb{R} \) as timeline: Does it serve as a good site for behaviors?
First guess: $\mathbb{R}$ as timeline

$\mathbb{R}$ as timeline: Does it serve as a good site for behaviors?
- What would a behavior type $B \in \text{Shv}(\mathbb{R})$ be?
  - On objects:
    - For each open interval $(a, b) \subseteq \mathbb{R}$, a set $B(a, b)$.
    - “The set of $B$-behaviors that can occur on $(a, b)$.”
First guess: \( \mathbb{R} \) as timeline

\( \mathbb{R} \) as timeline: Does it serve as a good site for behaviors?

- What would a behavior type \( B \in \text{Shv}(\mathbb{R}) \) be?
  - On objects:
    - For each open interval \((a, b) \subseteq \mathbb{R}\), a set \( B(a, b) \).
    - “The set of \( B \)-behaviors that can occur on \((a, b)\).”
  - On morphisms:
    - For each \( a \leq a' < b' \leq b \), a function \( B(a, b) \to B(a', b') \)
    - “The \( B \)-way to restrict \( B \)-behaviors over subintervals.”
First guess: \( \mathbb{R} \) as timeline

\( \mathbb{R} \) as timeline: Does it serve as a good site for behaviors?

- What would a behavior type \( B \in \text{Shv}(\mathbb{R}) \) be?
  - On objects:
    - For each open interval \((a, b) \subseteq \mathbb{R}\), a set \(B(a, b)\).
    - “The set of \(B\)-behaviors that can occur on \((a, b)\).”
  - On morphisms:
    - For each \(a \leq a' < b' \leq b\), a function \(B(a, b) \to B(a', b')\).
    - “The \(B\)-way to restrict \(B\)-behaviors over subintervals.”
  - Gluing conditions:
    - “Continuity”: \(B(a, b) = \lim_{a < a' < b' < b} B(a', b')\).
First guess: \( \mathbb{R} \) as timeline

\( \mathbb{R} \) as timeline: Does it serve as a good site for behaviors?

- What would a behavior type \( B \in \text{Shv}(\mathbb{R}) \) be?
  - On objects:
    - For each open interval \((a, b) \subseteq \mathbb{R}\), a set \( B(a, b) \).
    - “The set of \( B \)-behaviors that can occur on \((a, b)\).”
  - On morphisms:
    - For each \( a \leq a' < b' \leq b \), a function \( B(a, b) \rightarrow B(a', b') \).
    - “The \( B \)-way to restrict \( B \)-behaviors over subintervals.”
  - Gluing conditions:
    - “Continuity”: \( B(a, b) = \lim_{a < a' < b' < b} B(a', b') \).
    - “Composition”: \( B(a, b) = B(a, b') \times_{B(a', b')} B(a', b) \).
First guess: $\mathbb{R}$ as timeline

$\mathbb{R}$ as timeline: Does it serve as a good site for behaviors?

- What would a behavior type $B \in \text{Shv}(\mathbb{R})$ be?
  - On objects:
    - For each open interval $(a, b) \subseteq \mathbb{R}$, a set $B(a, b)$.
    - “The set of $B$-behaviors that can occur on $(a, b)$.”
  - On morphisms:
    - For each $a \leq a' < b' \leq b$, a function $B(a, b) \to B(a', b')$
    - “The $B$-way to restrict $B$-behaviors over subintervals.”
  - Gluing conditions:
    - “Continuity”: $B(a, b) = \lim_{a < a' < b' < b} B(a', b')$.
    - “Composition”: $B(a, b) = B(a, b') \times_{B(a', b')} B(a', b)$. 

![Graph](attachment:image.png)
First guess: \( \mathbb{R} \) as timeline

\( \mathbb{R} \) as timeline: Does it serve as a good site for behaviors?

- What would a behavior type \( B \in \text{Shv}(\mathbb{R}) \) be?
  - On objects:
    - For each open interval \( (a, b) \subseteq \mathbb{R} \), a set \( B(a, b) \).
    - “The set of \( B \)-behaviors that can occur on \( (a, b) \).”
  - On morphisms:
    - For each \( a \leq a' < b' \leq b \), a function \( B(a, b) \to B(a', b') \).
    - “The \( B \)-way to restrict \( B \)-behaviors over subintervals.”
  - Gluing conditions:
    - “Continuity”: \( B(a, b) = \lim_{a < a' < b' < b} B(a', b') \).
    - “Composition”: \( B(a, b) = B(a, b') \times_{B(a', b')} B(a', b) \).

\[ a \quad a' \quad b' \quad b \]
First guess: $\mathbb{R}$ as timeline

$\mathbb{R}$ as timeline: Does it serve as a good site for behaviors?

- What would a behavior type $B \in \text{Shv}(\mathbb{R})$ be?
  - On objects:
    - For each open interval $(a, b) \subseteq \mathbb{R}$, a set $B(a, b)$.
    - “The set of $B$-behaviors that can occur on $(a, b)$.”
  - On morphisms:
    - For each $a \leq a' < b' \leq b$, a function $B(a, b) \to B(a', b')$
    - “The $B$-way to restrict $B$-behaviors over subintervals.”

- Gluing conditions:
  - “Continuity”: $B(a, b) = \lim_{a < a' < b' < b} B(a', b')$.
  - “Composition”: $B(a, b) = B(a, b') \times_{B(a', b')} B(a', b)$. 

\[ a \quad a' \quad b' \quad b \]
Why \( \mathbb{R} \) is not preferable as the site

Two reasons *not to use* \( \text{Shv}(\mathbb{R}) \) as our topos.

1. Often want to consider **non-composable** behaviors!
   - “Roughly monotonic”: \( \forall (t_1, t_2). \ t_1 + 5 \leq t_2 \implies f(t_1) \leq f(t_2) \).
   - “Don’t move much”: \( \forall (t_1, t_2). \ -5 < f(t_1) - f(t_2) < 5 \).
   - Neither of these have the “composition gluing”.

2. Want to compare behavior across different time windows.
   - Example: a delay is “the same behavior at different times.”
   - \( \text{Shv}(\mathbb{R}) \) sees no relationship between \( B(0, 3) \) and \( B(2, 5) \).
   - Want “Translation invariance.”
   - Solution: Replace \( \mathbb{R} \) with an intervallic timeline.
   - Quotient by translation action.
Why $\mathbb{R}$ is not preferable as the site

Two reasons *not to use* $\text{Shv}(\mathbb{R})$ as our topos.

1. Often want to consider **non-composable** behaviors!
   - “Roughly monotonic”: $\forall (t_1, t_2). \ t_1 + 5 \leq t_2 \Rightarrow f(t_1) \leq f(t_2)$.
   - “Don’t move much”: $\forall (t_1, t_2). \ -5 < f(t_1) - f(t_2) < 5$.
   - Neither of these have the “composition gluing”.

2. Want to compare behavior across different time windows.
   - Example: a delay is “the same behavior at different times.”
   - $\text{Shv}(\mathbb{R})$ sees no relationship between $B(0, 3)$ and $B(2, 5)$. 
Why \( \mathbb{R} \) is not preferable as the site

Two reasons *not to use* \( \text{Shv}(\mathbb{R}) \) as our topos.

1. Often want to consider non-composable behaviors!
   - “Roughly monotonic”: \( \forall (t_1, t_2). t_1 + 5 \leq t_2 \Rightarrow f(t_1) \leq f(t_2) \).
   - “Don’t move much”: \( \forall (t_1, t_2). -5 < f(t_1) - f(t_2) < 5 \).
   - Neither of these have the “composition gluing”.

2. Want to compare behavior across different time windows.
   - Example: a delay is “the same behavior at different times.”
   - \( \text{Shv}(\mathbb{R}) \) sees no relationship between \( B(0, 3) \) and \( B(2, 5) \).
   - Want “Translation invariance.”
Why $\mathbb{R}$ is not preferable as the site

Two reasons *not to use* $\text{Shv}(\mathbb{R})$ as our topos.

1. Often want to consider **non-composable** behaviors!
   - “Roughly monotonic”: $\forall (t_1, t_2). \ t_1 + 5 \leq t_2 \Rightarrow f(t_1) \leq f(t_2)$.
   - “Don’t move much”: $\forall (t_1, t_2). \ -5 < f(t_1) - f(t_2) < 5$.
   - Neither of these have the “composition gluing”.

2. Want to compare behavior across different time windows.
   - Example: a delay is “the same behavior at different times.”
   - $\text{Shv}(\mathbb{R})$ sees no relationship between $B(0, 3)$ and $B(2, 5)$.
   - Want “Translation invariance.”

Solution:

- Replace $\mathbb{R}$ with an intervallic timeline.
- Quotient by translation action.
An intervallic time-line, $\mathbb{IR}$

For our timeline we use $\mathbb{IR}$ “the domain of real intervals”.
An intervallic time-line, $\mathbb{IR}$

For our timeline we use $\mathbb{IR}$ “the domain of real intervals”.

- **Definition** $\mathbb{IR} = \text{tw}(\mathbb{R}, \leq)^{\text{op}}$.
  - Points: $\{[a, b] \mid a \leq b \in \mathbb{R}\}$.
  - $[a, b] \subseteq [a', b']$ iff $a \leq a' \leq b' \leq b$.
  - $[a, b]$ is *less precise* than $[a', b']$.
  - $\mathbb{R} \subseteq \mathbb{IR}$ embeds as the maximal points, $[r, r]$. 
An intervallic time-line, $\mathbb{IR}$

For our timeline we use $\mathbb{IR}$ “the domain of real intervals”.

- Definition $\mathbb{IR} = \text{tw}(\mathbb{R}, \leq)^{\text{op}}$.
  - Points: $\{[a, b] \mid a \leq b \in \mathbb{R}\}$.
  - $[a, b] \subseteq [a’, b’]$ iff $a \leq a’ \leq b’ \leq b$.
  - $[a, b]$ is less precise than $[a’, b’]$.
  - $\mathbb{R} \subseteq \mathbb{IR}$ embeds as the maximal points, $[r, r]$.

- $\mathbb{IR}$ is a Scott domain:
  - Its poset of points determines a topology. How?
An intervallic time-line, $\mathbb{IR}$

For our timeline we use $\mathbb{IR}$ “the domain of real intervals”.

- **Definition** $\mathbb{IR} = \text{tw}(\mathbb{R}, \leq)^{\text{op}}$.
  - Points: $\{[a, b] \mid a \leq b \in \mathbb{R}\}$.
  - $[a, b] \subseteq [a', b']$ iff $a \leq a' \leq b' \leq b$.
  - $[a, b]$ is less precise than $[a', b']$.
  - $\mathbb{R} \subseteq \mathbb{IR}$ embeds as the maximal points, $[r, r]$.

- $\mathbb{IR}$ is a Scott domain:
  - Its poset of points determines a topology. How?
    - There’s are adjunctions $\mathbb{IR} \xleftarrow{\text{colim}} \xrightarrow{\text{Idl}(\mathbb{IR})} $.
      - $[a, b] \in \downarrow[a', b']$ iff $a < a' \leq b' < b$ (strict inequalities).
      - Scott topology: take as basis of opens $\{\uparrow[a, b] \mid a \leq b\}$. 
An intervallic time-line, $\mathbb{IR}$

For our timeline we use $\mathbb{IR}$ “the domain of real intervals”.

- Definition $\mathbb{IR} = \text{tw}(\mathbb{R}, \leq)^{\text{op}}$.
  - Points: $\{[a, b] \mid a \leq b \in \mathbb{R}\}$.
  - $[a, b] \subseteq [a’, b’]$ iff $a \leq a’ \leq b’ \leq b$.
  - $[a, b]$ is less precise than $[a’, b’]$.
  - $\mathbb{R} \subseteq \mathbb{IR}$ embeds as the maximal points, $[r, r]$.

- $\mathbb{IR}$ is a Scott domain:
  - Its poset of points determines a topology. How?

  There’s are adjunctions $\mathbb{IR} \xleftarrow{\text{colim}} \xrightarrow{\text{ldl}} \text{ldl}(\mathbb{IR})$.

  - $[a, b] \in \downarrow[a’, b’]$ iff $a < a’ \leq b’ < b$ (strict inequalities).
  - Scott topology: take as basis of opens $\{\uparrow[a, b] \mid a \leq b\}$.

This is our timeline: points are intervals.
Upper half-plane picture of $\mathbb{R}$

Topologically, we can represent $\mathbb{R}$ in the real upper half-plane.
Upper half-plane picture of $\mathbb{IR}$

Topologically, we can represent $\mathbb{IR}$ in the real upper half-plane.

Here is $\uparrow[a, b]$:
Upper half-plane picture of \( \mathbb{IR} \)

Topologically, we can represent \( \mathbb{IR} \) in the real upper half-plane.

- Here is \( \uparrow[a, b] \):

- Open sets \( U \in \text{Op}(\mathbb{IR}) \) are arbitrary unions of these.
- They have a nice characterization in terms of Lipschitz functions.
The topos $\mathcal{B}$ of behavior types

An intervallic time-line, $\mathbb{IR}$

Upper half-plane picture of $\mathbb{IR}$

Topologically, we can represent $\mathbb{IR}$ in the real upper half-plane.

- Here is $\uparrow[a, b]$:

![Diagram showing the upper half-plane picture of $\mathbb{IR}$]

- Open sets $U \in \text{Op}(\mathbb{IR})$ are arbitrary unions of these.
- They have a nice characterization in terms of Lipschitz functions.
  - $\{U_f \in \text{Op}(\mathbb{IR})\} \cong \{f : \mathbb{R} \to \mathbb{R}_+ \mid f \text{ is 1-Lipschitz}\}$.
  - Points under curve $f$ correspond to intervals (i.e. points) in $U_f$.

- These open sets will eventually be the truth-values in our topos.
Shv(IR): behaviors in the context of time

Each $X \in \text{Shv}(IR)$ is a behavior type occurring \textit{in the context of time}.

- IR is our (intervallic) time-line.
- $X[a, b]$ is the set of $X$-behaviors over the interval $[a, b]$.
- We can restrict behaviors to subintervals $a \leq a' \leq b' \leq b$. 
Shv(\(IR\)): behaviors in the context of time

Each \(X \in \text{Shv}(IR)\) is a behavior type occurring in the context of time.
- \(IR\) is our (intervallic) time-line.
- \(X[a, b]\) is the set of \(X\)-behaviors over the interval \([a, b]\).
- We can restrict behaviors to subintervals \(a \leq a' \leq b' \leq b\).

The truth-values in the topos \(\text{Shv}(IR)\) are Scott-open sets.
- The area under a 1-Lipschitz function is a Scott open.
- Truth of any proposition (e.g. “roughly monotonic”) is such an open.
  - Not “is its behavior roughly monotonic”?
Shv(\(\mathbb{IR}\)): behaviors in the context of time

Each \(X \in \text{Shv} (\mathbb{IR})\) is a behavior type occurring \textit{in the context of time.}

- \(\mathbb{IR}\) is our (intervallic) time-line.
- \(X[a, b]\) is the set of \(X\)-behaviors over the interval \([a, b]\).
- We can restrict behaviors to subintervals \(a \leq a' \leq b' \leq b\).

The truth-values in the topos \(\text{Shv} (\mathbb{IR})\) are Scott-open sets.

- The area under a 1-Lipschitz function is a Scott open.
- Truth of any proposition (e.g. “roughly monotonic”) is such an open.
  - Not “is its behavior roughly monotonic”?
  - But instead “over what intervals is it roughly monotonic”?

\(\text{Shv} (\mathbb{IR})\) is the topos of behavior types in the context of time.
Shv(\(\mathbb{IR}\)): behaviors in the context of time

Each \(X \in \text{Shv}(\mathbb{IR})\) is a behavior type occurring \textit{in the context of time}.

- \(\mathbb{IR}\) is our (intervallic) time-line.
- \(X[a, b]\) is the set of \(X\)-behaviors over the interval \([a, b]\).
- We can restrict behaviors to subintervals \(a \leq a' \leq b' \leq b\).

The truth-values in the topos \(\text{Shv}(\mathbb{IR})\) are Scott-open sets.

- The area under a 1-Lipschitz function is a Scott open.
- Truth of any proposition (e.g. “roughly monotonic”) is such an open.
  - Not “is its behavior roughly monotonic”?
  - But instead “over what intervals is it roughly monotonic”?

\(\text{Shv}(\mathbb{IR})\) is the topos of behavior types in the context of time.

Next up: keep durations, remove fixed timeline.
Translation-invariant quotient topos $\mathcal{B}$

We want translation-invariance to compare behaviors over different times.
Translation-invariant quotient topos \( \mathcal{B} \)

We want translation-invariance to compare behaviors over different times.

- Translation action \( \mathbb{R} \xrightarrow{\oplus} \text{Aut}(\mathbb{R}) \), \( r \triangleright [a, b] := [a + r, b + r] \)
Translation-invariant quotient topos \( \mathcal{B} \)

We want translation-invariance to compare behaviors over different times.

- Translation action \( \mathbb{R} \xrightarrow{\triangleright} \text{Aut}(\mathbb{R}), \quad r \triangleright [a, b] := [a + r, b + r] \)
- This induces a *left-exact comonad* \( T \) on \( \text{Shv}(\mathbb{R}) \).
  - (Left-exact comonads are what define geometric surjections.)
  - For \( X \in \text{Shv}(\mathbb{R}) \), define \( TX \in \text{Shv}(\mathbb{R}) \) by
    \[
    (TX)[a, b] := \prod_{r \in \mathbb{R}} X[a + r, b + r].
    \]
Translation-invariant quotient topos $\mathcal{B}$

We want translation-invariance to compare behaviors over different times.

- Translation action $\mathbb{R} \xrightarrow{\rightharpoonup} \text{Aut}(\mathbb{IR})$, $r \rightharpoonup [a, b] := [a + r, b + r]$.
- This induces a left-exact comonad $T$ on $\text{Shv}(\mathbb{IR})$.
  - (Left-exact comonads are what define geometric surjections.)
  - For $X \in \text{Shv}(\mathbb{IR})$, define $TX \in \text{Shv}(\mathbb{IR})$ by
    \[(TX)[a, b] := \prod_{r \in \mathbb{R}} X[a + r, b + r].\]
- $T$-coalgebras are translation-equivariant sheaves.
- Define topos $\mathcal{B} := T\text{-coAlg}$ of “behavior types”.
- In fact $\mathcal{B}$ is an étendue.
Translation-invariant quotient topos $\mathcal{B}$

We want translation-invariance to compare behaviors over different times.

- Translation action $\mathbb{R} \rightarrow \text{Aut}(\mathbb{IR})$, $r \triangleright [a, b] := [a + r, b + r]$
- This induces a *left-exact comonad* $T$ on $\text{Shv}(\mathbb{IR})$.
  - (Left-exact comonads are what define geometric surjections.)
  - For $X \in \text{Shv}(\mathbb{IR})$, define $TX \in \text{Shv}(\mathbb{IR})$ by
    $$(TX)[a, b] := \prod_{r \in \mathbb{R}} X[a + r, b + r].$$
- $T$-coalgebras are translation-equivariant sheaves.
- Define topos $\mathcal{B} := T\text{-coAlg}$ of “behavior types”.
- In fact $\mathcal{B}$ is an étendue.
  - There is an inhabited object, which we call $\text{Time} \in \mathcal{B}$,
  - And an equivalence $\text{Shv}(\mathbb{IR}) \cong \mathcal{B}/\text{Time}$.
  - Makes precise “$\text{Shv}(\mathbb{IR})$ is behavior types in the context of time.”
Translation-invariant quotient topos $\mathcal{B}$

We want translation-invariance to compare behaviors over different times.

- Translation action $\mathbb{R} \to \text{Aut}(\mathbb{IR})$, $r \triangleright [a, b] := [a + r, b + r]$
- This induces a *left-exact comonad* $T$ on $\text{Shv}(\mathbb{IR})$.
  - (Left-exact comonads are what define geometric surjections.)
  - For $X \in \text{Shv}(\mathbb{IR})$, define $TX \in \text{Shv}(\mathbb{IR})$ by
    $$(TX)[a, b] := \prod_{r \in \mathbb{R}} X[a + r, b + r].$$

- $T$-coalgebras are translation-equivariant sheaves.
- Define topos $\mathcal{B} := T$-coAlg of “behavior types”.  
- In fact $\mathcal{B}$ is an étendue.
  - There is an inhabited object, which we call $\text{Time} \in \mathcal{B}$, 
  - And an equivalence $\text{Shv}(\mathbb{IR}) \cong \mathcal{B}/\text{Time}$.  
  - Makes precise “$\text{Shv}(\mathbb{IR})$ is behavior types in the context of time.”

Next we’ll give a site presentation of this topos $\mathcal{B}$.
A site for $\mathcal{B}$

Consider the twisted-arrow category $\mathbb{I}\mathbb{R}/\triangleright = \text{tw}(\mathbb{R}_{\geq 0})$.

- **Objects** = $\{\ell \in \mathbb{R}_{\geq 0}\}$.
- **Hom$(\ell', \ell)$** = $\{\langle r, s \rangle \mid r + \ell' + s = \ell\}^2$

---

$\mathbb{I}\mathbb{R}/\triangleright$ is a continuous category in the sense of Johnstone-Joyal.

Coverage $\{\langle r, s \rangle : \ell' \rightarrow \ell \mid r > 0, s > 0\}$.

When $r, s > 0$, write $\ell' \dashv\rightarrow \ell$.

The topos of behavior types: $\mathcal{B} = \text{Shv}(\mathbb{I}\mathbb{R}/\triangleright)$.

A sheaf $X$ assigns a set of possible behaviors to each $\ell$ and a restriction map to each included subinterval $\langle r, s \rangle : \ell' \rightarrow \ell$ such that $X(\ell)$ limits $\ell' \dashv\rightarrow \ell$.

Étendue means “extent”; $\mathbb{I}\mathbb{R}/\triangleright$ is indeed extents (durations) of time.

Lawvere also studied sheaves on $\mathbb{I}\mathbb{R}/\triangleright$, but used “composition gluing” whereas we use “continuity gluing.”
A site for $\mathcal{B}$

Consider the twisted-arrow category $\mathbb{IR}/\triangleright = \text{tw}(\mathbb{R}_{\geq 0})$.

- Objects $= \{ \ell \in \mathbb{R}_{\geq 0} \}$.
- $\text{Hom}(\ell', \ell) = \{ \langle r, s \rangle \mid r + \ell' + s = \ell \}$

$\mathbb{IR}/\triangleright$ is a continuous category in the sense of Johnstone-Joyal.

- Coverage $\{ \langle r, s \rangle : \ell' \to \ell \mid r > 0, s > 0 \}$.
- When $r, s > 0$, write $\ell' \rightsquigarrow \ell$.

The topos of behavior types: $\mathcal{B} \cong \text{Shv}(\mathbb{IR}/\triangleright)$

\textsuperscript{2}Lawvere also studied sheaves on $\mathbb{IR}/\triangleright$, but used “composition gluing” whereas we use “continuity gluing.”
A site for $\mathcal{B}$

Consider the twisted-arrow category $\mathbb{IR}/\triangleright = \text{tw}(\mathbb{R}_{\geq 0})$.

- Objects $= \{\ell \in \mathbb{R}_{\geq 0}\}$.
- $\text{Hom}(\ell', \ell) = \{\langle r, s \rangle \mid r + \ell' + s = \ell\}^2$

$\mathbb{IR}/\triangleright$ is a continuous category in the sense of Johnstone-Joyal.

- Coverage $\{\langle r, s \rangle \colon \ell' \to \ell \mid r > 0, s > 0\}$.
- When $r, s > 0$, write $\ell' \leadsto \ell$.

The topos of behavior types: $\mathcal{B} \cong \text{Shv}(\mathbb{IR}/\triangleright)$

- A sheaf $X$ assigns a set of possible behaviors to each $\ell$,
- And a restriction map to each included subinterval $\langle r, s \rangle \colon \ell' \to \ell$,
- Such that $X(\ell) \cong \lim_{\ell' \leadsto \ell} X(\ell')$.

---

$^2$Lawvere also studied sheaves on $\mathbb{IR}/\triangleright$, but used “composition gluing” whereas we use “continuity gluing.”
A site for $\mathcal{B}$

Consider the twisted-arrow category $\mathbb{IR}/\triangleright = \text{tw}(\mathbb{R}_{\geq 0})$.

- Objects $= \{\ell \in \mathbb{R}_{\geq 0}\}$.
- $\text{Hom}(\ell', \ell) = \{\langle r, s \rangle \mid r + \ell' + s = \ell\}$

$\mathbb{IR}/\triangleright$ is a continuous category in the sense of Johnstone-Joyal.

- Coverage $\{\langle r, s \rangle \colon \ell' \to \ell \mid r > 0, s > 0\}$.
- When $r, s > 0$, write $\ell' \rightsquigarrow \ell$.

The topos of behavior types: $\mathcal{B} \cong \text{Shv}(\mathbb{IR}/\triangleright)$

- A sheaf $X$ assigns a set of possible behaviors to each $\ell$,
- And a restriction map to each included subinterval $\langle r, s \rangle \colon \ell' \to \ell$,
- Such that $X(\ell) \cong \lim_{\ell' \rightsquigarrow \ell} X(\ell')$.

Étendue means “extent”; $\mathbb{IR}/\triangleright$ is indeed extents (durations) of time.

---

\(^2\)Lawvere also studied sheaves on $\mathbb{IR}/\triangleright$, but used “composition gluing” whereas we use “continuity gluing.”
Example behavior types $X \in \mathcal{B}$

We contend that any sort of behavior can be modeled as an object $X \in \mathcal{B}$. 
Example behavior types $X \in \mathcal{B}$

We contend that any sort of behavior can be modeled as an object $X \in \mathcal{B}$.

- Trajectories through a vector field,
- Delays (+ delay differential equations),
- Stochastic walk through a graph,
- $\Omega$: subobject classifier is “1-Lipschitz functions”.

\begin{itemize}
  \item \includegraphics[width=\textwidth]{vector_field}
  \item \includegraphics[width=\textwidth]{graph_diagram}
\end{itemize}
Example behavior types $X \in \mathcal{B}$

We contend that any sort of behavior can be modeled as an object $X \in \mathcal{B}$.

- Trajectories through a vector field,
- Delays (+ delay differential equations),
- Stochastic walk through a graph,
- $\Omega$: subobject classifier is “1-Lipschitz functions”.

Next up: want logic to define other interesting behaviors.
Logical expressions give amazingly convenient representations.

- “Whenever I touch blue, I’ll spend 1 full sec. on blue within 5 sec’s.”
- $\forall (t : \text{Time}). \bigwedge_{[0,0]}^t B(x) \Rightarrow \exists (r : \mathbb{R}). 0 \leq r \leq 5 \land \bigwedge_{[r,r+1]}^t B(x)$. 

Kripke-Joyal semantics

Logical expressions like the above can be interpreted in the topos $\mathcal{B}$. E.g. the above defines a map $P : X \rightarrow \Omega$, given $B : X \rightarrow \Omega$. This in turn gives a subtype $\{ X | P \}$ of "P-good behavior".

How is internal logic convenient?

- compact notation,
- precise semantics,
- quite expressive,
- readable in natural language, e.g. English.
Preview of higher-order temporal logic for behavior

Logical expressions give amazingly convenient representations.

- “Whenever I touch blue, I’ll spend 1 full sec. on blue within 5 sec’s.”
- $\forall (t : \text{Time}). \exists (r : \mathbb{R}). 0 \leq r \leq 5 \land \forall_{[t,t+1]} B(x)$.

Kripke-Joyal semantics

- Logical expressions like the above can be interpreted in the topos $\mathcal{B}$.
- E.g. the above defines a map $P : X \rightarrow \Omega$, given $B : X \rightarrow \Omega$.
- This in turn gives a subtype $\{ X \mid P \}$ of “$P$-good behavior”.
Preview of higher-order temporal logic for behavior

Logical expressions give amazingly convenient representations.
- “Whenever I touch blue, I’ll spend 1 full sec. on blue within 5 sec’s.”
- $\forall (t : \text{Time}). \exists (r : \mathbb{R}). 0 \leq r \leq 5 \land \forall_{[r, r+1]} B(x)$.

Kripke-Joyal semantics
- Logical expressions like the above can be interpreted in the topos $\mathcal{B}$.
- E.g. the above defines a map $P : X \to \Omega$, given $B : X \to \Omega$.
- This in turn gives a subtype $\{X | P\}$ of “$P$-good behavior”.

How is internal logic is convenient?
- compact notation,
- precise semantics,
- quite expressive,
- readable in natural language, e.g. English.
Outline

1. Introduction

2. The topos $\mathcal{B}$ of behavior types

3. Temporal type theory
   - Toposes, type theory, and logic
   - A finitely-presented language with semantics in $\mathcal{B}$
   - Local reals and derivatives

4. Application to the NAS

5. Conclusion

Internal language of a topos

The internal language—previewed above—does a lot of heavy lifting.

3Étendues are “locally locales”, so we can use locale terminology, like “open subset”.

**Internal language of a topos**

The internal language—previewed above—does a lot of heavy lifting.

- Here is *Kripke-Joyal semantics* for a sheaf topos.

<table>
<thead>
<tr>
<th>Logical expr.</th>
<th>Sheaf-theoretic translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\forall (x : X). P(x)$</td>
<td>For all open $U$, and all $x \in X(U)$, $P\big</td>
</tr>
<tr>
<td>$\exists (x : X). P(x)$</td>
<td>There is an open cover $(U_i)_{i \in I}$ and a section $x \in X(U_i)$ in each, s.t. $P\big</td>
</tr>
<tr>
<td>$P \Rightarrow Q$</td>
<td>For all open $U$, if $P\big</td>
</tr>
<tr>
<td>$P \lor Q$</td>
<td>There is an open cover $(U_i)_{i \in I}$, s.t. $P\big</td>
</tr>
<tr>
<td>etc.</td>
<td>etc.</td>
</tr>
</tbody>
</table>

---

3 Étendues are “locally locales”, so we can use locale terminology, like “open subset”. 
Internal language of a topos

The internal language—previewed above—does a lot of heavy lifting.

- Here is *Kripke-Joyal semantics* for a sheaf topos.

<table>
<thead>
<tr>
<th>Logical expr.</th>
<th>Sheaf-theoretic translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\forall (x : X). P(x)$</td>
<td>For all open $U$, and all $x \in X(U)$, $P</td>
</tr>
<tr>
<td>$\exists (x : X). P(x)$</td>
<td>There is an open cover $(U_i)_{i \in I}$ and a section $x \in X(U_i)$ in each, s.t. $P</td>
</tr>
<tr>
<td>$P \Rightarrow Q$</td>
<td>For all open $U$, if $P</td>
</tr>
<tr>
<td>$P \lor Q$</td>
<td>There is an open cover $(U_i)_{i \in I}$, s.t. $P</td>
</tr>
<tr>
<td>etc.</td>
<td>etc.</td>
</tr>
</tbody>
</table>

(In $\mathcal{B}$, all covers are filtered, so $\lor$ degenerates: no need for cover.)

---

$^3$Étendues are “locally locales”, so we can use locale terminology, like “open subset”.
Example: Dedekind numeric objects

In any sheaf topos, use logic to define various Dedekind numeric objects.
Example: Dedekind numeric objects

In any sheaf topos, use logic to define various *Dedekind numeric objects*.

- Start with $\mathbb{Q}$; its semantics is the constant sheaf $\mathbb{Q}$.
- Consider functions $\delta : \mathbb{Q} \to \Omega$ (“the lower bounds” for some real).
- We can define the *lower reals* internally:

$$\mathbb{R} := \{ \delta : \mathbb{Q} \to \Omega \mid \exists q. \delta q \land \forall q. \delta q \iff \exists q'. q < q' \land \delta q' \}.$$
Example: Dedekind numeric objects

In any sheaf topos, use logic to define various *Dedekind numeric objects*.

- Start with $\mathbb{Q}$; its semantics is the constant sheaf $\mathbb{Q}$.
- Consider functions $\delta : \mathbb{Q} \to \Omega$ ("the lower bounds" for some real).
- We can define the *lower reals* internally:

  $$\mathbb{R} := \{ \delta : \mathbb{Q} \to \Omega \mid \exists q. \delta q \land \forall q. \delta q \iff \exists q'. q < q' \land \delta q' \}.$$  

  - The semantics are nice on localic toposes. If $X$ is a top. sp., $\llbracket \mathbb{R} \rrbracket (U) = \{ \text{lower semi-continuous functions } U \to \mathbb{R} \}$. 
  
  - Dually, define $\bar{\mathbb{R}}$, with $\llbracket \bar{\mathbb{R}} \rrbracket (U) = \{ \text{upper semi-continuous} \ldots \}$.
Example: Dedekind numeric objects

In any sheaf topos, use logic to define various *Dedekind numeric objects*.

- Start with $\mathbb{Q}$; its semantics is the constant sheaf $\mathbb{Q}$.
- Consider functions $\delta : \mathbb{Q} \to \Omega$ (“the lower bounds” for some real).
- We can define the *lower reals* internally:

\[
\bar{\mathbb{R}} := \{ \delta : \mathbb{Q} \to \Omega \mid \exists q. \delta q \land \forall q. \delta q \iff \exists q'. \, q < q' \land \delta q' \}.
\]

- The semantics are nice on localic toposes. If $X$ is a top. sp.,
  \[ \llbracket \bar{\mathbb{R}} \rrbracket(U) = \{ \text{lower semi-continuous functions} \, U \to \mathbb{R} \} \].
- Dually, define $\bar{\bar{\mathbb{R}}}$, with $\llbracket \bar{\bar{\mathbb{R}}} \rrbracket(U) = \{ \text{upper semi-continuous} \ldots \}$
- $\bar{\bar{\mathbb{R}}} := \bar{\mathbb{R}} \times \bar{\mathbb{R}}$: *extended intervals*.
- $\mathbb{R} := \{(\delta, \nu) : \bar{\bar{\mathbb{R}}} \mid \forall q. \neg(\delta q \land \nu q) \land \forall(q < q'). \delta q \lor \nu q' \}$. 

We refer to all of these as *Dedekind numeric objects*. 
Example: Dedekind numeric objects

In any sheaf topos, use logic to define various Dedekind numeric objects.

- Start with $\mathbb{Q}$; its semantics is the constant sheaf $\mathbb{Q}$.
- Consider functions $\delta : \mathbb{Q} \to \Omega$ (“the lower bounds” for some real).
- We can define the lower reals internally:

$$\mathbb{R} := \{ \delta : \mathbb{Q} \to \Omega \mid \exists q. \delta q \land \forall q. \delta q \iff \exists q'. q < q' \land \delta q' \}.$$ 

- The semantics are nice on localic toposes. If $X$ is a top. sp.,
- $\llbracket \mathbb{R} \rrbracket (U) = \{ \text{lower semi-continuous functions } U \to \mathbb{R} \}$. 

- Dually, define $\bar{\mathbb{R}}$, with $\llbracket \bar{\mathbb{R}} \rrbracket (U) = \{ \text{upper semi-continuous . . . } \}$
- $\bar{\mathbb{R}} := \mathbb{R} \times \bar{\mathbb{R}}$: extended intervals.
- $\mathbb{R} := \{ (\delta, \nu) : \bar{\mathbb{R}} \mid \forall q. \neg(\delta q \land \nu q) \land \forall (q < q'). \delta q \lor \nu q' \}$. 

We refer to all of these as Dedekind numeric objects.
What is temporal type theory?

Temporal type theory: a finitely presented sublanguage of $\mathcal{B}$’s language.

- The internal language of $\mathcal{B}$ is infinite:
  - It consists of every object (as type), morphism (as term),
  - every commutative diagram, finite limit, exp’l object, etc. in $\mathcal{B}$. 
Temporal type theory: a finitely presented sublanguage of $\mathcal{B}$’s language.

- The internal language of $\mathcal{B}$ is infinite:
  - It consists of every object (as type), morphism (as term),
  - every commutative diagram, finite limit, exp’l object, etc. in $\mathcal{B}$.

- What if we want non-topos-theorists to use this formal system?
  - NASA uses formal methods to prove properties of systems.
  - These are formulas and proofs written in (temporal) logic.
  - We want same, but with richer type system, better semantics.
Temporal type theory: a finitely presented sublanguage of $\mathcal{B}$’s language.

- The internal language of $\mathcal{B}$ is infinite:
  - It consists of every object (as type), morphism (as term),
  - every commutative diagram, finite limit, exp’l object, etc. in $\mathcal{B}$.

- What if we want non-topos-theorists to use this formal system?
  - NASA uses *formal methods* to prove properties of systems.
  - These are formulas and proofs written in (temporal) logic.
  - We want same, but with richer type system, better semantics.

- We present a finite sub-language; build what we need from within. This finite sublanguage is what we call *temporal type theory*. 
Temporal type theory

The finitely presented language has:

- One atomic predicate symbol, \( \text{unit\_speed}: \mathbb{R} \to \Omega \).
The finitely presented language has:

- One atomic predicate symbol, \( \text{unit\_speed} : \mathbb{R} \rightarrow \Omega \).

- From here, define \( \text{Time} := \{ x : \mathbb{R} \mid \text{unit\_speed}(x) \} \).

- Idea: internalize the set of time-lines (clock behaviors).
  - What is a clock behavior (on an external interval)?
  - It is an internal interval, moving along at unit speed.
Temporal type theory

The finitely presented language has:
- One atomic predicate symbol, \( \text{unit\_speed} : \mathbb{R} \rightarrow \Omega \).
- From here, define \( \text{Time} := \{ x : \mathbb{R} | \text{unit\_speed}(x) \} \).
- Idea: internalize the set of time-lines (clock behaviors).
- What is a clock behavior (on an external interval)?
  - It is an internal interval, moving along at unit speed.
- The theory has ten axioms, e.g. that \( \text{Time} \) is an \( \mathbb{R} \)-torsor:
  - \( \forall (t : \text{Time})(r : \mathbb{R}). t + r \in \text{Time} \),
  - \( \forall (t_1, t_2 : \text{Time}). \exists! (r : \mathbb{R}). t_1 + r = t_2 \).
Temporal type theory

The finitely presented language has:
- One atomic predicate symbol, \( \text{unit\_speed} : \mathbb{R} \to \Omega \).
  - From here, define \( \text{Time} := \{ x : \mathbb{R} \mid \text{unit\_speed}(x) \} \).
  - Idea: internalize the set of time-lines (clock behaviors).
    - What is a clock behavior (on an external interval)?
    - It is an internal interval, moving along at unit speed.

- The theory has ten axioms, e.g. that \( \text{Time} \) is an \( \mathbb{R} \)-torsor:
  - \( \forall (t : \text{Time})(r : \mathbb{R}). t + r \in \text{Time} \),
  - \( \forall (t_1, t_2 : \text{Time}). \exists! (r : \mathbb{R}). t_1 + r = t_2 \).

Sound semantics in \( \mathcal{B} \):
- We already had \( \text{Time} \in \mathcal{B} \) externally.
- Check that with that interpretation, the ten axioms hold.
Aside: relation to other temporal logics

There are other, widely used, temporal logics.

- They involve modalities like “Until” and “Since”.
- Completeness results like Kamp’s theorem:
  - Equivalence with “first-order monadic logic of order” $FO(\prec)$

Monadic doesn’t mean monad, it means there is one type: Time, and every predicate symbol is unary $P(t)$ only.

Time is ordered: we have a relation $\prec$ on Time.

The logic is otherwise first-order and boolean.

Example: $\forall t. P(t) \Rightarrow \exists t'. t < t' \land Q(t)$.

TTT is pretty different: it’s a type theory; we have many different types (sheaves).

We have a higher order logic, with no “monadic”-type restrictions.

We can embed $FO(\prec)$ into our language (just $\neg\neg$ everything).

Trade-off: TTT is much more expressive; much less “automatable.”
Aside: relation to other temporal logics

There are other, widely used, temporal logics.
- They involve modalities like “Until” and “Since”.
- Completeness results like Kamp’s theorem:
  - Equivalence with “first-order monadic logic of order” $FO(<)$
    - Monadic doesn’t mean monad,
    - It means there is one type: $\text{Time}$,
    - And every predicate symbol is unary $P(t)$ only.
    - Time is ordered: we have a relation $<$ on $\text{Time}$.
    - The logic is otherwise first-order and boolean.
- Example: $\forall t. P(t) \Rightarrow \exists t’. t < t’ \land Q(t)$. 
Aside: relation to other temporal logics

There are other, widely used, temporal logics.

- They involve modalities like “Until” and “Since”.
- Completeness results like Kamp’s theorem:
  - Equivalence with “first-order monadic logic of order” $FO(<)$
    - Monadic doesn’t mean monad,
    - It means there is one type: $\text{Time}$,
    - And every predicate symbol is unary $P(t)$ only.
    - Time is ordered: we have a relation $<$ on $\text{Time}$.
    - The logic is otherwise first-order and boolean.
  - Example: $\forall t. P(t) \Rightarrow \exists t'. t < t' \land Q(t)$.

TTT is pretty different:

- It’s a type theory; we have many different types (sheaves).
- We have a higher order logic, with no “monadic”-type restrictions.
- We can embed $FO(<)$ into our language (just $\neg\neg$ everything).
- Trade-off: TTT is much more expressive; much less “automatable”.
Temporal type theory

A finitely-presented language with semantics in $\mathcal{B}$

Modalities, $@$ and $\pi$

There are a number of useful modalities (Lawvere-Tierney topologies).

- Modalities are internal monads $j : \Omega \to \Omega$.
  - That is, $P \Rightarrow jP$, $jjP \Rightarrow jP$, $j(P \land Q) \iff (jP \land jQ)$.
  - One-to-one correspondence $\{\text{modalities}\} \cong \{\text{subtoposes}\}$.
Modalities, \(\mathcal{O}\) and \(\pi\)

There are a number of useful modalities (Lawvere-Tierney topologies).

- Modalities are internal monads \(j : \Omega \rightarrow \Omega\).
- That is, \(P \Rightarrow jP\), \(jjP \Rightarrow jP\), \(j(P \land Q) \Leftrightarrow (jP \land jQ)\).
- One-to-one correspondence \(
\{\text{modalities}\} \cong \{\text{subtoposes}\}\).

Example 1,2: in the context of \(t : \text{Time}\), have \(\downarrow^t_{[a,b]}\), \(\mathcal{O}^t_{[a,b]} : \Omega \rightarrow \Omega\).

- \(\downarrow^t_{[a,b]}P := P \lor (a < t \lor t < b)\).
- \(\mathcal{O}^t_{[a,b]}P := (P \Rightarrow (a < t \lor t < b)) \Rightarrow (a < t \lor t < b)\).

These are hard to read, but correspond to useful subtoposes:

- \(\mathcal{O}^t_{[a,b]}\) corresponds to single point subtopos \([a, b]\) \(\subseteq \mathbb{IR}\).
- \(\downarrow^t_{[a,b]}\) corresponds to its closure \(\downarrow [a, b] \subseteq \mathbb{IR}\).
Modalities, $\odot$ and $\pi$

There are a number of useful modalities (Lawvere-Tierney topologies).

- Modalities are internal monads $j : \Omega \to \Omega$.
- That is, $P \Rightarrow jP, \quad jjP \Rightarrow jP, \quad j(P \land Q) \leftrightarrow (jP \land jQ)$.
- One-to-one correspondence $\{\text{modalities}\} \cong \{\text{subtoposes}\}$.

Example 1,2: in the context of $t : \text{Time}$, have $\downarrow_{[a,b]}^t, \odot_{[a,b]}^t : \Omega \to \Omega$.

- $\downarrow_{[a,b]}^t P := P \lor (a < t \lor t < b)$.
- $\odot_{[a,b]}^t P := (P \Rightarrow (a < t \lor t < b)) \Rightarrow (a < t \lor t < b)$.

These are hard to read, but correspond to useful subtoposes:

- $\odot_{[a,b]}^t$ corresponds to single point subtopos $\{[a, b]\} \subseteq \mathbb{IR}$.
- $\downarrow_{[a,b]}^t$ corresponds to its closure $\downarrow [a, b] \subseteq \mathbb{IR}$.

Example 3: In empty context we have $\pi : \Omega \to \Omega$.

- $\pi P := \forall (t : \text{Time}). \odot_{[0,0]}^t P$.
- Corresponds to the dense subtopos $\mathbb{R}/\searrow \subseteq \mathbb{IR}/\searrow$. 
Modalities, \( \Box \) and \( \pi \)

There are a number of useful modalities (Lawvere-Tierney topologies).

- Modalities are internal monads \( j : \Omega \to \Omega \).
  - That is, \( P \Rightarrow jP, \; jjP \Rightarrow jP, \; j(P \land Q) \iff (jP \land jQ) \).
  - One-to-one correspondence \( \{ \text{modalities} \} \cong \{ \text{subtoposes} \} \).

- Example 1,2: in the context of \( t : \text{Time} \), have \( \downarrow^t_{[a,b]}, \Box^t_{[a,b]} : \Omega \to \Omega \).
  - \( \downarrow^t_{[a,b]} P := P \lor (a < t \lor t < b) \).
  - \( \Box^t_{[a,b]} P := (P \Rightarrow (a < t \lor t < b)) \Rightarrow (a < t \lor t < b) \).
  - These are hard to read, but correspond to useful subtoposes:
    - \( \Box^t_{[a,b]} \) corresponds to single point subtopos \( \{ [a, b] \} \subseteq \mathbb{R} \).
    - \( \downarrow^t_{[a,b]} \) corresponds to its closure \( \downarrow [a, b] \subseteq \mathbb{R} \).

- Example 3: In empty context we have \( \pi : \Omega \to \Omega \).
  - \( \pi P := \forall (t : \text{Time}). \Box^t_{[0,0]} P \).
  - Corresponds to the dense subtopos \( \mathbb{R}/_\triangleright \subseteq \mathbb{IR}/_\triangleright \).

We can use these modalities to define local Dedekind numeric types.
Local Dedekind numeric types

For any $j$, we can define $\mathbb{R}_j, \bar{\mathbb{R}}_j, \bar{\bar{\mathbb{R}}}_j, \mathbb{R}_j$, etc.
Local Dedekind numeric types

For any $j$, we can define $\mathbb{R}_j$, $\mathbb{R}_\bar{\迄今}$, $\mathbb{R}_{\bar{\迄今}}$, $\mathbb{R}_j$, etc.

- $j$-logic: replace all connectives/quantifiers with their $j$-counterparts.
  - Each connective / quantifier satisfies a universal property,
  - Want same univ. property on $j$-closed propositions $P, Q \in \Omega_j$.
  - I.e. reflect logic of $j$-subtopos $\mathcal{B}_j$ into $\mathcal{B}$.
  - Example: define $j$-logic versions of Dedekind numeric types.
Local Dedekind numeric types

For any $j$, we can define $\mathbb{R}_j, \bar{\mathbb{R}}_j, \tilde{\mathbb{R}}_j, \mathbb{R}_j$, etc.

- $j$-logic: replace all connectives/quantifiers with their $j$-counterparts.
  - Each connective / quantifier satisfies a universal property,
  - Want same univ. property on $j$-closed propositions $P, Q \in \Omega_j$.
  - I.e. reflect logic of $j$-subtopos $\mathcal{B}_j$ into $\mathcal{B}$.
  - Example: define $j$-logic versions of Dedekind numeric types.

- $\mathbb{R}_j := \{ \delta : \mathbb{Q} \to \Omega_j \mid j\exists q. \delta q \land \forall q. \delta q \iff j\exists q'. q < q' \land \delta q' \}$
  - When $j = \text{id}$ this is lower semicontinuous fns on $\mathbb{IR}$.
  - When $j = \pi$, it’s lower semicontinuous fns on $\mathbb{R}$.
  - When $j = @^t_{[a,b]}$, it’s lower semicontinuous fns on a point.
Local Dedekind numeric types

For any $j$, we can define $\mathbb{R}_j$, $\mathbb{R}_j$, $\mathbb{R}_j$, $\mathbb{R}_j$, etc.

- $j$-logic: replace all connectives/quantifiers with their $j$-counterparts.
  - Each connective / quantifier satisfies a universal property,
  - Want same univ. property on $j$-closed propositions $P, Q \in \Omega_j$.
  - I.e. reflect logic of $j$-subtopos $\mathcal{B}_j$ into $\mathcal{B}$.
  - Example: define $j$-logic versions of Dedekind numeric types.

- $\mathbb{R}_j := \{ \delta : \mathbb{Q} \rightarrow \Omega_j \mid j \exists q. \delta q \land \forall q. \delta q \leftrightarrow j \exists q'. q < q' \land \delta q' \}$
  - When $j = \text{id}$ this is lower semicontinuous fns on $\mathbb{IR}$.
  - When $j = \pi$, it’s lower semicontinuous fns on $\mathbb{R}$.
  - When $j = \circ^t_{[a,b]}$, it’s lower semicontinuous fns on a point.

Now we are equipped to define derivatives.
Derivatives of continuous reals

We can define derivatives internally.

- Semantics of $x : \mathbb{R}_\pi$ is continuous function of (pointwise) time.
- Evaluation of $x$ at a point $r : \mathbb{R}$ is given by $\mathbb{R}[r]x \in \mathbb{R}[r,r]$
- We denote this $x^\@ (r)$.
Derivatives of continuous reals

We can define derivatives internally.

- Semantics of \( x : \mathbb{R}_\pi \) is continuous function of (pointwise) time.
  - Evaluation of \( x \) at a point \( r : \mathbb{R} \) is given by \( \circ \left[ r, r \right] x \in \mathbb{R} \circ \left[ r, r \right] \)
  - We denote this \( x^{\circ}(r) \).

- We define the derivative of any interval function \( x : \overline{\mathbb{R}}_\pi \).
  - Result is another interval function \( \dot{x} : \overline{\mathbb{R}}_\pi \), namely:
  - \( q_1 < \dot{x} < q_2 \) iff for all \( r_1 < r_2 : \mathbb{R} \),
    \[
    q_1 \ll \frac{x^{\circ}(r_2) - x^{\circ}(r_1)}{r_2 - r_1} \ll q_2.
    \]
Derivatives of continuous reals

We can define derivatives internally.

- Semantics of $x : \mathbb{R}_\pi$ is continuous function of (pointwise) time.
  - Evaluation of $x$ at a point $r : \mathbb{R}$ is given by $\circ_{[r,r]} x \in \mathbb{R} \circ_{[r,r]}$
  - We denote this $x^@ (r)$.

- We define the derivative of any interval function $x : \overline{\mathbb{R}}_\pi$.
  - Result is another interval function $\dot{x} : \overline{\mathbb{R}}_\pi$, namely:
    - $q_1 < \dot{x} < q_2$ iff for all $r_1 < r_2 : \mathbb{R}$,
      $$q_1 \ll \frac{x^@ (r_2) - x^@ (r_1)}{r_2 - r_1} \ll q_2.$$

- Theorem: $\dot{x}$ internally is linear in $x$ and satisfies Leibniz rule.
Derivatives of continuous reals

We can define derivatives internally.

- Semantics of $x : \mathbb{R}_\pi$ is continuous function of (pointwise) time.
  - Evaluation of $x$ at a point $r : \mathbb{R}$ is given by $\odot_{[r,r]} x \in \mathbb{R} \odot[r,r]$.
  - We denote this $x^\odot(r)$.

- We define the derivative of any interval function $x : \bar{\mathbb{R}}_\pi$.
  - Result is another interval function $\dot{x} : \bar{\mathbb{R}}_\pi$, namely:
    - $q_1 < \dot{x} < q_2$ iff for all $r_1 < r_2 : \mathbb{R}$,
      $$ q_1 \ll \frac{x^\odot(r_2) - x^\odot(r_1)}{r_2 - r_1} \ll q_2. $$

- Theorem: $\dot{x}$ internally is linear in $x$ and satisfies Leibniz rule.
- Theorem: $\dot{x}$ externally has semantics of derivative of $x$.
  - Caveat: $\dot{x}$ is defined for any cts $x$, even if non-differentiable.
Derivatives of continuous reals

We can define derivatives internally.

- Semantics of $x : \mathbb{R}_\pi$ is continuous function of (pointwise) time.
  - Evaluation of $x$ at a point $r : \mathbb{R}$ is given by $\circ_{[r,r]}^\circ \in \mathbb{R} \circ_{[r,r]}$.
  - We denote this $x^\circ(r)$.
- We define the derivative of any interval function $x : \mathbb{R}_\pi$.
  - Result is another interval function $\dot{x} : \mathbb{R}_\pi$, namely:
    - $q_1 < \dot{x} < q_2$ iff for all $r_1 < r_2 : \mathbb{R}$,
      $$ q_1 \ll \frac{x^\circ(r_2) - x^\circ(r_1)}{r_2 - r_1} \ll q_2. $$

- Theorem: $\dot{x}$ internally is linear in $x$ and satisfies Leibniz rule.
- Theorem: $\dot{x}$ externally has semantics of derivative of $x$.
  - Caveat: $\dot{x}$ is defined for any cts $x$, even if non-differentiable.
  - When $x$ is externally differentiable, $\dot{x}$ is its derivative.
  - When not, $\dot{x}$ is interval-valued “very reasonable” notion.
Differential equations

As a logical expression, derivatives work like anything else.

Consider a differential equation, like

\[ f(\dot{x}, \ddot{x}, a, b) = 0. \]
Differential equations

As a logical expression, derivatives work like anything else.

- Consider a differential equation, like

\[ f(\dot{x}, \ddot{x}, a, b) = 0. \]

- Maybe \( a, b : \mathbb{R}_{\pi} \) are continuous functions of time.
- Regardless, \( f(\dot{x}, \ddot{x}, a, b) = 0 \) is just an equation in the logic.
  - Use it with \( \top, \bot, \neg, \lor, \land, \Rightarrow, \exists, \forall \).
  - Can be combined with any other property.
Outline

1. Introduction
2. The topos $\mathcal{B}$ of behavior types
3. Temporal type theory
4. Application to the NAS
   - A simplified case
   - Combining local contracts for safety guarantee
5. Conclusion

Simplifying the safe separation problem.

- Real problem: safe separation for pairs of planes.
- Components: Radars, pilots, thrusters/actuators.
- Behavior types: Discrete signals, (continuous) diff-eqs, delays.
The problem: safe altitude

Simplifying the safe separation problem.
- Real problem: safe separation for pairs of planes.
  - Components: Radars, pilots, thrusters/actuators.
  - Behavior types: Discrete signals, (continuous) diff-eqs, delays.
- Simplification: safe altitude for one plane.
  - One radar, one pilot, one thruster.
  - Same behavior types: discrete, continuous, delay.
The problem: safe altitude

Simplifying the safe separation problem.

- Real problem: safe separation for pairs of planes.
  - Components: Radars, pilots, thrusters/actuators.
  - Behavior types: Discrete signals, (continuous) diff-eqs, delays.
- Simplification: safe altitude for one plane.
  - One radar, one pilot, one thruster.
  - Same behavior types: discrete, continuous, delay.

Goal: combine disparate guarantees to prove useful result.
Setup

Variables to be used, and their types:

\[ t : \text{Time}. \quad T, P : \text{Cmd}. \quad a : \mathbb{R}_\pi. \quad \text{safe, margin, del, rate} : \mathbb{Q}. \]

What these mean:

- \( t : \text{Time.} \) time-line (a clock).
- \( a : \mathbb{R}_\pi. \) altitude (continuously changing).
- \( T : \text{Cmd.} \) TCAS command (occurs at discrete instants).
- \( P : \text{Cmd.} \) pilot’s command (occurs at discrete instants).
- \( \text{safe} : \mathbb{Q}. \) safe altitude (constant).
- \( \text{margin} : \mathbb{Q}. \) margin-of-error (constant).
- \( \text{del} : \mathbb{Q}. \) pilot delay (constant).
- \( \text{rate} : \mathbb{Q}. \) maximal ascent rate (constant).

Behavior contracts

- $t : \text{Time.}$ 
  - time-line 
  - (a clock).
- $a : \mathbb{R}^\pi.$ 
  - altitude 
  - (continuously changing).
- $T : \text{Cmd.}$ 
  - TCAS command 
  - (occurs at discrete instants).
- $P : \text{Cmd.}$ 
  - pilot’s command 
  - (occurs at discrete instants).
- $\text{safe} : Q.$ 
  - safe altitude 
  - (constant).
- $\text{margin} : Q.$ 
  - margin-of-error 
  - (constant).
- $\text{del} : Q.$ 
  - pilot delay 
  - (constant).
- $\text{rate} : Q.$ 
  - maximal ascent rate 
  - (constant).

- $\theta_1 := (\text{margin} > 0) \land (a \geq 0).$
Behavior contracts

- $t : \text{Time.}$  
- $a : \mathbb{R}^\tau.$  
- $T : \text{Cmd.}$  
- $P : \text{Cmd.}$  
- $\text{safe} : \mathbb{Q}.$  
- $\text{margin} : \mathbb{Q}.$  
- $\text{del} : \mathbb{Q}.$  
- $\text{rate} : \mathbb{Q}.$  

- $\theta_1 := (\text{margin} > 0) \land (a \geq 0).$
- $\theta_2 := (a > \text{safe} + \text{margin} \Rightarrow T = \text{level}).$
- $\theta'_2 := (a < \text{safe} + \text{margin} \Rightarrow T = \text{climb}).$
Behavior contracts

- \( t : \text{Time.} \): time-line (a clock).
- \( a : \mathbb{R}_{\pi}. \): altitude (continuously changing).
- \( T : \text{Cmd.} \): TCAS command (occurs at discrete instants).
- \( P : \text{Cmd.} \): pilot’s command (occurs at discrete instants).
- \( \text{safe} : \mathbb{Q}. \): safe altitude (constant).
- \( \text{margin} : \mathbb{Q}. \): margin-of-error (constant).
- \( \text{del} : \mathbb{Q}. \): pilot delay (constant).
- \( \text{rate} : \mathbb{Q}. \): maximal ascent rate (constant).

\[
\begin{align*}
\theta_1 &:= (\text{margin} > 0) \land (a \geq 0). \\
\theta_2 &:= (a > \text{safe} + \text{margin} \Rightarrow T = \text{level}). \\
\theta'_2 &:= (a < \text{safe} + \text{margin} \Rightarrow T = \text{climb}). \\
\theta_3 &:= (P = \text{level} \Rightarrow \dot{a} = 0) \land (P = \text{climb} \Rightarrow \dot{a} = \text{rate}).
\end{align*}
\]
Behavior contracts

- \( t : \text{Time.} \) : time-line (a clock).
- \( a : \mathbb{R}_{≠} \) : altitude (continuously changing).
- \( T : \text{Cmd.} \) : TCAS command (occurs at discrete instants).
- \( P : \text{Cmd.} \) : pilot’s command (occurs at discrete instants).
- \( \text{safe} : \mathbb{Q.} \) : safe altitude (constant).
- \( \text{margin} : \mathbb{Q.} \) : margin-of-error (constant).
- \( \text{del} : \mathbb{Q.} \) : pilot delay (constant).
- \( \text{rate} : \mathbb{Q.} \) : maximal ascent rate (constant).

- \( θ_1 := (\text{margin} > 0) ∧ (a ≥ 0). \)
- \( θ_2 := (a > \text{safe} + \text{margin} \Rightarrow T = \text{level}). \)
- \( θ_2' := (a < \text{safe} + \text{margin} \Rightarrow T = \text{climb}). \)
- \( θ_3 := (P = \text{level} \Rightarrow \dot{a} = 0) ∧ (P = \text{climb} \Rightarrow \dot{a} = \text{rate}). \)
- \( θ_4 := \text{is_delayed}(\text{del}, T, P). \)

\( θ_4 \) is an abbreviation for a longer logical condition.
Behavior contracts

- $t : \text{Time.}$ time-line (a clock).
- $a : \mathbb{R}_+. \quad \text{altitude (continuously changing).}$
- $T : \text{Cmd.} \quad \text{TCAS command (occurs at discrete instants).}$
- $P : \text{Cmd.} \quad \text{pilot's command (occurs at discrete instants).}$
- safe : $Q. \quad \text{safe altitude (constant).}$
- margin : $Q. \quad \text{margin-of-error (constant).}$
- del : $Q. \quad \text{pilot delay (constant).}$
- rate : $Q. \quad \text{maximal ascent rate (constant).}$

- $\theta_1 := (\text{margin} > 0) \land (a \geq 0).$
- $\theta_2 := (a > \text{safe} + \text{margin} \Rightarrow T = \text{level}).$
- $\theta'_2 := (a < \text{safe} + \text{margin} \Rightarrow T = \text{climb}).$
- $\theta_3 := (P = \text{level} \Rightarrow \dot{a} = 0) \land (P = \text{climb} \Rightarrow \dot{a} = \text{rate}).$
- $\theta_4 := \text{is\_delayed}(\text{del}, T, P).$

$\theta_4$ is an abbreviation for a longer logical condition.

- Can prove safe separation
  $$\forall(t : \text{Time}). \, \downarrow_{0}^{t}(t > \text{del} + \frac{\text{safe}}{\text{rate}} \Rightarrow a \geq \text{safe}).$$
Outline

1. Introduction
2. The topos $\mathcal{B}$ of behavior types
3. Temporal type theory
4. Application to the NAS
5. Conclusion
   - Summary
   - Further reading

*Temporal Type Theory*, https://arxiv.org/abs/1710.10258
Summary

Summary

- Many different formalisms for behavior, but they all occur in time.
  - We say that time occurs in intervals, which can be restricted.
  - Sheaves are behavior types: “what can occur over intervals.”
Idea: topos theory for integrating systems in a big tent framework.

Many different formalisms for behavior, but they all occur in time.
- We say that time occurs in intervals, which can be restricted.
- Sheaves are behavior types: “what can occur over intervals.”

The topos has a native “internal” logic.
- Looks like usual set theory, ∀, ∃, ∧, ∨, ⇒, ¬; use formal methods.
- Has built-in Time object: do temporal logic.
- Internal definition of ODEs, hybrid systems, etc.
- Logically prove sheaf-theoretic behavioral properties.

This temporal type theory is quite general, and fully compositional.
If you’re interested in reading more

- Book (to be published by Springer Berkhäuser).
  - *Temporal Type Theory.*
  - Technical parts, some friendly parts.

Questions and comments are welcome. Thanks!
If you’re interested in reading more

- Book (to be published by Springer Berkhaüser).
  - *Temporal Type Theory*.
  - Freely available: https://arxiv.org/abs/1710.10258
  - Technical parts, some friendly parts.

- Book (probably to be published by Cambridge University Press).
  - *Seven Sketches in Compositionality*.
  - Freely available: https://arxiv.org/abs/1803.05316
  - Chapter 7 is about this material.
  - Friendly!
If you’re interested in reading more

- Book (to be published by Springer Berkhäuser).
  - *Temporal Type Theory.*
  - Freely available: https://arxiv.org/abs/1710.10258
  - Technical parts, some friendly parts.

- Book (probably to be published by Cambridge University Press).
  - *Seven Sketches in Compositionality.*
  - Freely available: https://arxiv.org/abs/1803.05316
  - Chapter 7 is about this material.
  - Friendly!

*Questions and comments are welcome. Thanks!*