A topos-theoretic approach to systems and behavior

David I. Spivak* and Patrick Schultz

Mathematics Department
Massachusetts Institute of Technology

Category Theory Conference
2018/07/09

Outline

An example system

The National Airspace System (NAS)

- 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]

[1] Traffic Collision Avoidance System.

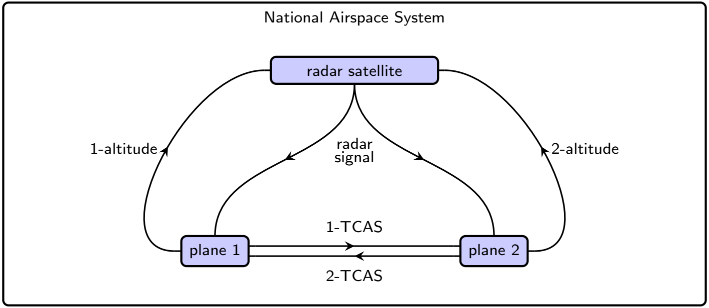
An example system

The National Airspace System (NAS)

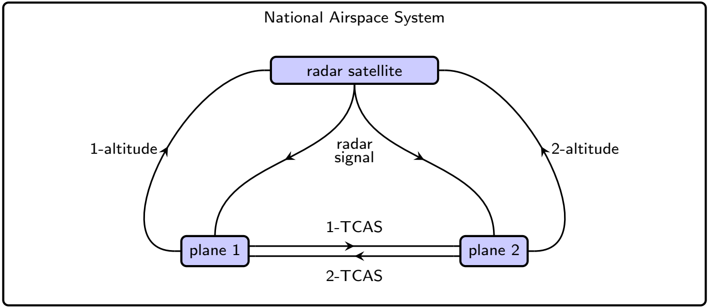
- Safe separation problem:
  - Planes need to remain at a safe distance.
  - Can't generally communicate directly.
  - Use radars, pilots, ground control, radios, and TCAS.[1]
- Systems of systems:
  - A great variety of interconnected systems.
  - Work in concert to enforce global property: safe separation.

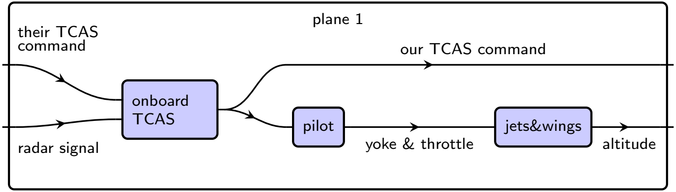
[1] Traffic Collision Avoidance System.

Systems of interacting systems in the NAS

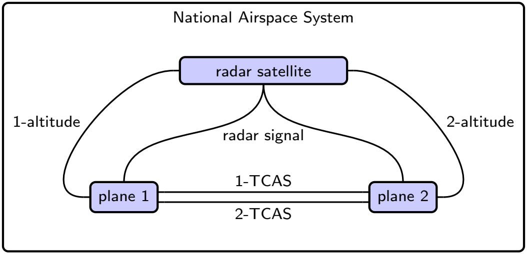


Systems of interacting systems in the NAS





Behavior contracts as predicates

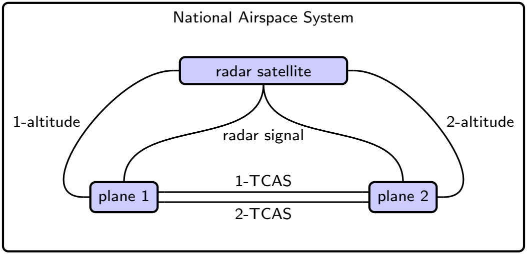


We assign to each...

- ... wire: a sheaf.
- ... box: a predicate—a behavior contract—on the product of its wires.

Prove that if each box's predicate is satisfied, safe separation is achieved.

Behavior contracts as predicates



We assign to each...

- ... wire: a sheaf.
- ... box: a predicate—a behavior contract—on the product of its wires.

Prove that if each box's predicate is satisfied, safe separation is achieved.

We'll discuss such a situation using topos theory.

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.

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 so engineers can prove safety of combined systems.

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 so engineers can prove safety of combined systems.

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 a NAS use-case.

Outline

What is behavior?

We want to model various types of behavior.

- 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 various types of behavior.

- 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?

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 $B \in \mathrm{Shv}(\mathbb{R})$ 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 $B \in \mathsf{Shv}(\mathbb{R})$ 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 $B(a, b) \to B(a', b')$.
    - Restriction: "watch a clip of the movie".

First guess: $\mathbb{R}$ as timeline

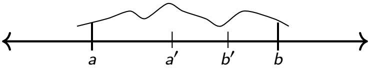
$\mathbb{R}$ as timeline: Does it serve as a good site for behaviors?

- What would a behavior type $B \in \mathrm{Shv}(\mathbb{R})$ 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 $B(a, b) \longrightarrow B(a', b')$.
    - Restriction: "watch a clip of the movie".
  - 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 $B \in \mathrm{Shv}(\mathbb{R})$ 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 $B(a, b) \to B(a', b')$.
    - Restriction: "watch a clip of the movie".
  - Gluing conditions:
    - "Continuity": $B(a, b) = \lim_{a<a'<b'<b} B(a', b')$.
    - "Composition": $B(a, b) = B(a, b') \times_{B(a',b')} B(a', b)$.



Why $\mathbb{R}$ is not preferable as the site

Two reasons *not to use* $\mathrm{Shv}(\mathbb{R})$ 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 satisfy “composition gluing”.

Why $\mathbb{R}$ is not preferable as the site

Two reasons *not to use* 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 satisfy "composition gluing".
- 2. Want to compare behavior across different time windows.
  - Example: a delay is "the same behavior at different times."
  - 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* $\mathrm{Shv}(\mathbb{R})$ 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 satisfy "composition gluing".
- 2. Want to compare behavior across different time windows.
  - Example: a delay is "the same behavior at different times."
  - $\mathrm{Shv}(\mathbb{R})$ sees no relationship between $B(0,3)$ and $B(2,5)$.
  - We want "Translation invariance."

Why $\mathbb{R}$ is not preferable as the site

Two reasons *not to use* $\mathrm{Shv}(\mathbb{R})$ 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 satisfy "composition gluing".
- 2. Want to compare behavior across different time windows.
  - Example: a delay is "the same behavior at different times."
  - $\mathrm{Shv}(\mathbb{R})$ sees no relationship between $B(0, 3)$ and $B(2, 5)$.
  - We want "Translation invariance."

Solution:

- Replace $\mathbb{R}$ with an intervallic timeline, and...
- ... quotient by translation action.

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

For our timeline we use $\mathbb{IR}$ "the interval domain".

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

For our timeline we use $\mathbb{IR}$ "the interval domain".

- Definition $\mathbb{IR} = \mathrm{tw}(\mathbb{R}, \leq)^{\mathrm{op}}$.
  - Points: $\{[a, b] \mid a \leq b \in \mathbb{R}\}$.
  - $[a, b] \sqsubseteq [a', b']$ 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 interval domain".

- Definition $\mathbb{IR} = \mathrm{tw}(\mathbb{R}, \leq)^{\mathrm{op}}$.
  - Points: $\{[a, b] \mid a \leq b \in \mathbb{R}\}$.
  - $[a, b] \sqsubseteq [a', b']$ 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...
  - ...for which $\sqsubseteq$ is specialization order on points.
  - Basis: open intervals (a, b), denoting $\{[a', b'] \mid a < a' \leq b' < b\}$.

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

For our timeline we use $\mathbb{IR}$ "the interval domain".

- Definition $\mathbb{IR} = \mathrm{tw}(\mathbb{R}, \leq)^{\mathrm{op}}$.
  - Points: $\{[a, b] \mid a \leq b \in \mathbb{R}\}$.
  - $[a, b] \sqsubseteq [a', b']$ 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...
  - ...for which $\sqsubseteq$ is specialization order on points.
  - Basis: open intervals (a, b), denoting $\{[a', b'] \mid a < a' \leq b' < b\}$.

This space, $\mathbb{IR}$ is our timeline, and its points are intervals.

$\mathrm{Shv}(\mathbb{IR})$: behaviors in the context of time

Each $X \in \mathrm{Shv}(\mathbb{IR})$ is a behavior type occurring *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 $a \leq a' \leq b' \leq b$.
- And behaviors satisfy "continuity gluing,"

$$X(a,b) \cong \lim_{a<a'<b'<b} X(a',b').$$

Shv($\mathbb{IR}$): behaviors in the context of time

Each $X \in \mathrm{Shv}(\mathbb{IR})$ is a behavior type occurring *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 $a \leq a' \leq b' \leq b$.
- And behaviors satisfy "continuity gluing,"

$$X(a, b) \cong \lim_{a<a'<b'<b} X(a', b').$$

Next up: keep durations, drop the 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 $\mathbb{R} \xrightarrow{\triangleright} \mathrm{Aut}(\mathbb{IR})$, $\quad r \triangleright (a, b) := (a + r, b + r)$

Translation-invariant quotient topos $\mathcal{B}$

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

- Translation action $\mathbb{R} \xrightarrow{\triangleright} \mathrm{Aut}(\mathbb{IR})$, $\quad r \triangleright (a, b) := (a + r, b + r)$
- This induces a *left-exact comonad* T on $\mathrm{Shv}(\mathbb{IR})$.
  - (Left-exact comonads are what define quotient toposes.)
  - For $X \in \mathrm{Shv}(\mathbb{IR})$, define $TX \in \mathrm{Shv}(\mathbb{IR})$ 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 $\mathbb{R} \xrightarrow{\triangleright} \mathrm{Aut}(\mathbb{IR})$, $\quad r \triangleright (a, b) := (a + r, b + r)$
- This induces a *left-exact comonad* T on $\mathrm{Shv}(\mathbb{IR})$.
  - (Left-exact comonads are what define quotient toposes.)
  - For $X \in \mathrm{Shv}(\mathbb{IR})$, define $TX \in \mathrm{Shv}(\mathbb{IR})$ 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, meaning...

Translation-invariant quotient topos $\mathcal{B}$

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

- Translation action $\mathbb{R} \xrightarrow{\triangleright} \mathrm{Aut}(\mathbb{IR})$, $\quad r \triangleright (a, b) := (a + r, b + r)$
- This induces a *left-exact comonad* T on $\mathrm{Shv}(\mathbb{IR})$.
  - (Left-exact comonads are what define quotient toposes.)
  - For $X \in \mathrm{Shv}(\mathbb{IR})$, define $TX \in \mathrm{Shv}(\mathbb{IR})$ 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, meaning...
  - There is an inhabited object, which we call $\mathtt{Time} \in \mathcal{B}$,
  - And an equivalence $\mathrm{Shv}(\mathbb{IR}) \cong \mathcal{B}/\mathtt{Time}$.
  - Makes precise "$\mathrm{Shv}(\mathbb{IR})$ is behavior types in the context of time."

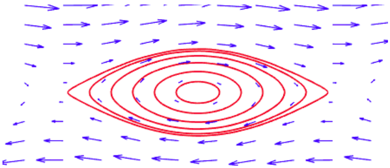
Example behavior types $X \in \mathcal{B}$

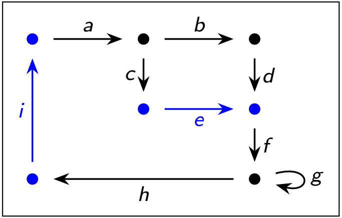
We contend that any sort of behavior can be modeled as an object $X \in \mathcal{B}$.

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: "labeled transition system".

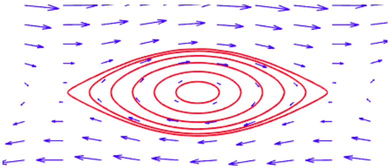


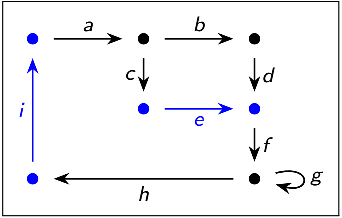


Example behavior types $X \in \mathcal{B}$

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: "labeled transition system".





Next up: want logic to define other interesting behaviors.

- "Whenever I touch blue, I'll spend 1 full sec. on blue within 5 sec's."

Preview of higher-order temporal logic for behavior

In any topos, logical expressions are amazingly convenient.

- "Whenever I touch blue, I'll spend 1 full sec. on blue within 5 sec's."
- $\forall(t : \mathtt{Time}).\, @^t_{[0,0]} B(x) \Rightarrow \exists(r : \mathbb{R}).\, 0 \leq r \leq 5 \wedge @^t_{[r,r+1]} B(x).$

Preview of higher-order temporal logic for behavior

In any topos, logical expressions are amazingly convenient.

- "Whenever I touch blue, I'll spend 1 full sec. on blue within 5 sec's."
- $\forall(t : \texttt{Time}).\, @^{t}_{[0,0]}B(x) \Rightarrow \exists(r : \mathbb{R}).\, 0 \leq r \leq 5 \wedge @^{t}_{[r,r+1]}B(x).$

Kripke-Joyal semantics

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

Preview of higher-order temporal logic for behavior

In any topos, logical expressions are amazingly convenient.

- "Whenever I touch blue, I'll spend 1 full sec. on blue within 5 sec's."
- $\forall(t : \mathtt{Time}).\, @^t_{[0,0]}B(x) \Rightarrow \exists(r : \mathbb{R}).\, 0 \leq r \leq 5 \wedge @^t_{[r,r+1]}B(x)$.

Kripke-Joyal semantics

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

How is internal logic is convenient?

- compact notation,
- precise semantics,
- quite expressive,
- readable in natural language, e.g. English.

Preview of higher-order temporal logic for behavior

In any topos, logical expressions are amazingly convenient.

- "Whenever I touch blue, I'll spend 1 full sec. on blue within 5 sec's."
- $\forall(t : \texttt{Time}).\, @^t_{[0,0]} B(x) \Rightarrow \exists(r : \mathbb{R}).\, 0 \leq r \leq 5 \wedge @^t_{[r,r+1]} B(x).$

Kripke-Joyal semantics

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

How is internal logic is convenient?

- compact notation,
- precise semantics,
- quite expressive,
- readable in natural language, e.g. English.

Next: use logic to define real "numbers".

Outline

Dedekind numeric objects

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

Dedekind numeric objects

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

- Start with $\mathbb{Q}$; it's semantically the constant sheaf $\mathbb{Q}$.
- Think of a function $L : \mathbb{Q} \to \Omega$ as the "$\mathbb{Q}$-lower bounds" for a real.
- We can define the type $\underline{\mathbb{R}}$ of *lower reals* internally:

$$\underline{\mathbb{R}} \coloneqq \{L : \mathbb{Q} \to \Omega \mid \exists q.\, Lq \wedge \forall q.\, Lq \Leftrightarrow \exists q'.\, q < q' \wedge Lq'\}.$$

Dedekind numeric objects

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

- Start with $\mathbb{Q}$; it's semantically the constant sheaf $\mathbb{Q}$.
- Think of a function $L : \mathbb{Q} \to \Omega$ as the "$\mathbb{Q}$-lower bounds" for a real.
- We can define the type $\underline{\mathbb{R}}$ of *lower reals* internally:

$$\underline{\mathbb{R}} \coloneqq \{L : \mathbb{Q} \to \Omega \mid \exists q.\, Lq \wedge \forall q.\, Lq \Leftrightarrow \exists q'.\, q < q' \wedge Lq'\}.$$

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

Dedekind numeric objects

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

- Start with $\mathbb{Q}$; it's semantically the constant sheaf $\mathbb{Q}$.
- Think of a function $L : \mathbb{Q} \to \Omega$ as the "$\mathbb{Q}$-lower bounds" for a real.
- We can define the type $\underline{\mathbb{R}}$ of *lower reals* internally:

$$\underline{\mathbb{R}} := \{L : \mathbb{Q} \to \Omega \mid \exists q.\, Lq \wedge \forall q.\, Lq \Leftrightarrow \exists q'.\, q < q' \wedge Lq'\}.$$

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

- Dually, define $\bar{\mathbb{R}}$, with $[\![\, \bar{\mathbb{R}} \,]\!](U) = \{\text{upper semi-continuous} \ldots\}$
- $\underline{\bar{\mathbb{R}}} := \underline{\mathbb{R}} \times \bar{\mathbb{R}}$: *extended intervals*.
- $\mathbb{R} := \{(L, R) : \underline{\bar{\mathbb{R}}} \mid \forall q.\, \neg(Lq \wedge Rq) \wedge \forall (q < q').\, Lq \vee Rq'\}$.

Dedekind numeric objects

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

- Start with $\mathbb{Q}$; it's semantically the constant sheaf $\mathbb{Q}$.
- Think of a function $L : \mathbb{Q} \to \Omega$ as the "$\mathbb{Q}$-lower bounds" for a real.
- We can define the type $\underline{\mathbb{R}}$ of *lower reals* internally:

$$\underline{\mathbb{R}} \coloneqq \{L : \mathbb{Q} \to \Omega \mid \exists q.\, Lq \wedge \forall q.\, Lq \Leftrightarrow \exists q'.\, q < q' \wedge Lq'\}.$$

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

- Dually, define $\overline{\mathbb{R}}$, with $[\![\overline{\mathbb{R}}]\!](U) = \{\text{upper semi-continuous} \ldots\}$
- $\overline{\underline{\mathbb{R}}} \coloneqq \underline{\mathbb{R}} \times \overline{\mathbb{R}}$: *extended intervals.*
- $\mathbb{R} \coloneqq \{(L, R) : \overline{\underline{\mathbb{R}}} \mid \forall q.\, \neg(Lq \wedge Rq) \wedge \forall (q < q').\, Lq \vee Rq'\}$.

We refer to $\underline{\mathbb{R}}, \overline{\mathbb{R}}, \overline{\underline{\mathbb{R}}}, \mathbb{R}$, etc. as *Dedekind numeric objects*.

Temporal type theory

TTT is a finitely presented sub-language of $\mathcal{B}$'s internal language:

- One atomic predicate symbol, $\mathrm{unit\_speed}\colon \bar{\underline{\mathbb{R}}} \to \Omega$.

Temporal type theory

TTT is a finitely presented sub-language of $\mathcal{B}$'s internal language:

- One atomic predicate symbol, $\mathrm{unit\_speed}\colon \underline{\bar{\mathbb{R}}} \to \Omega$.
    - From here, define $\mathtt{Time} := \{\, t : \underline{\bar{\mathbb{R}}} \mid \mathrm{unit\_speed}(t) \,\}$.
    - Note that we can treat times $t : \mathtt{Time}$ as real intervals.

Temporal type theory

TTT is a finitely presented sub-language of $\mathcal{B}$'s internal language:

- One atomic predicate symbol, $\mathrm{unit\_speed}\colon \bar{\underline{\mathbb{R}}} \to \Omega$.
  - From here, define $\mathtt{Time} := \{\, t : \bar{\underline{\mathbb{R}}} \mid \mathrm{unit\_speed}(t) \,\}$.
  - Note that we can treat times $t : \mathtt{Time}$ as real intervals.

TTT axiomatics: find finitely many axioms with which to "do real work".

- Ten axioms, e.g. that Time is an $\mathbb{R}$-torsor:
  - $\forall(t : \mathtt{Time})(r : \mathbb{R}).\ t + r \in \mathtt{Time}$,
  - $\forall(t_1, t_2 : \mathtt{Time}).\ \exists!(r : \mathbb{R}).\ t_1 + r = t_2$.

Temporal type theory

TTT is a finitely presented sub-language of $\mathcal{B}$'s internal language:

- One atomic predicate symbol, $\mathrm{unit\_speed}\colon \bar{\underline{\mathbb{R}}} \to \Omega$.
  - From here, define $\mathtt{Time} := \{\, t : \bar{\underline{\mathbb{R}}} \mid \mathrm{unit\_speed}(t) \,\}$.
  - Note that we can treat times $t : \mathtt{Time}$ as real intervals.

TTT axiomatics: find finitely many axioms with which to "do real work".

- Ten axioms, e.g. that Time is an $\mathbb{R}$-torsor:
  - $\forall (t : \mathtt{Time})(r : \mathbb{R}).\ t + r \in \mathtt{Time}$,
  - $\forall (t_1, t_2 : \mathtt{Time}).\ \exists!(r : \mathbb{R}).\ t_1 + r = t_2$.
- All are sound in $\mathcal{B}$
  - We already had $\mathtt{Time} \in \mathcal{B}$ externally in the éntendue $\mathcal{B}$.
  - Check that with that interpretation, the ten axioms hold.

Modalities, @ and π

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

- Modalities are internal monads $j\colon \Omega \to \Omega$ on the subobject classifier.
  - That is, $P \Rightarrow jP, \quad jjP \Rightarrow jP, \quad j(P \wedge Q) \Leftrightarrow (jP \wedge jQ)$.
  - One-to-one correspondence $\{\text{modalities}\} \cong \{\text{subtoposes}\}$.

Modalities, @ and π

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

- Modalities are internal monads $j\colon \Omega \to \Omega$ on the subobject classifier.
  - That is, $P \Rightarrow jP, \quad jjP \Rightarrow jP, \quad j(P \wedge Q) \Leftrightarrow (jP \wedge jQ)$.
  - One-to-one correspondence $\{\text{modalities}\} \cong \{\text{subtoposes}\}$.
- Example 1,2: in the context of $t : \mathtt{Time}$, have modalities $\downarrow^t_{[a,b]}, @^t_{[a,b]}$.
  - $\downarrow^t_{[a,b]} P := P \vee (a < t \vee t < b)$.
  - $@^t_{[a,b]} P := (P \Rightarrow (a < t \vee t < b)) \Rightarrow (a < t \vee t < b)$.
  - These are hard to read, but correspond to useful subtoposes:
    - $@^t_{[a,b]}$ 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, @ and π

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

- Modalities are internal monads $j\colon \Omega \to \Omega$ on the subobject classifier.
  - That is, $P \Rightarrow jP, \quad jjP \Rightarrow jP, \quad j(P \wedge Q) \Leftrightarrow (jP \wedge jQ)$.
  - One-to-one correspondence $\{\text{modalities}\} \cong \{\text{subtoposes}\}$.
- Example 1,2: in the context of $t : \mathtt{Time}$, have modalities $\downarrow^t_{[a,b]}$, $@^t_{[a,b]}$.
  - $\downarrow^t_{[a,b]} P := P \vee (a < t \vee t < b)$.
  - $@^t_{[a,b]} P := (P \Rightarrow (a < t \vee t < b)) \Rightarrow (a < t \vee t < b)$.
  - These are hard to read, but correspond to useful subtoposes:
    - $@^t_{[a,b]}$ corresponds to single point subtopos $\{[a,b]\} \subseteq \mathbb{IR}$.
    - $\downarrow^t_{[a,b]}$ corresponds to its closure $\downarrow[a,b] \subseteq \mathbb{IR}$.
- Example 3: We have "pointwise" modality π.
  - $\pi P := \forall (t : \mathtt{Time}).\, @^t_{[0,0]} P$.
  - Corresponds to the dense subtopos $\mathbb{R} \subseteq \mathbb{IR}$.

Modalities, @ and π

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

- Modalities are internal monads $j\colon \Omega \to \Omega$ on the subobject classifier.
  - That is, $P \Rightarrow jP, \quad jjP \Rightarrow jP, \quad j(P \wedge Q) \Leftrightarrow (jP \wedge jQ)$.
  - One-to-one correspondence $\{\text{modalities}\} \cong \{\text{subtoposes}\}$.
- Example 1,2: in the context of $t : \mathtt{Time}$, have modalities $\downarrow^t_{[a,b]}, @^t_{[a,b]}$.
  - $\downarrow^t_{[a,b]} P := P \vee (a < t \vee t < b)$.
  - $@^t_{[a,b]} P := (P \Rightarrow (a < t \vee t < b)) \Rightarrow (a < t \vee t < b)$.
  - These are hard to read, but correspond to useful subtoposes:
    - $@^t_{[a,b]}$ corresponds to single point subtopos $\{[a,b]\} \subseteq \mathbb{IR}$.
    - $\downarrow^t_{[a,b]}$ corresponds to its closure $\downarrow [a,b] \subseteq \mathbb{IR}$.
- Example 3: We have "pointwise" modality π.
  - $\pi P := \forall (t : \mathtt{Time}).\, @^t_{[0,0]} P$.
  - Corresponds to the dense subtopos $\mathbb{R} \subseteq \mathbb{IR}$.

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

Local Dedekind numeric types

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

Local Dedekind numeric types

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

- $\underline{\mathbb{R}}_j := \{L\colon \mathbb{Q} \to \Omega_j \mid j\exists q.\, Lq \wedge \forall q.\, Lq \Leftrightarrow j\exists q'.\, q < q' \wedge Lq'\}$
  - When $j = \mathrm{id}$ this is lower semicontinuous fns on $\mathbb{IR}$.
  - When $j = \pi$, it's lower semicontinuous fns on $\mathbb{R} \subseteq \mathbb{IR}$.
  - When $j = @^t_{[a,b]}$, it's lower semicontinuous fns on a point.

Local Dedekind numeric types

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

- $\underline{\mathbb{R}}_j := \{L \colon \mathbb{Q} \to \Omega_j \mid j\exists q.\, Lq \land \forall q.\, Lq \Leftrightarrow j\exists q'.\, q < q' \land Lq'\}$
  - When $j = \mathrm{id}$ this is lower semicontinuous fns on $\mathbb{IR}$.
  - When $j = \pi$, it's lower semicontinuous fns on $\mathbb{R} \subseteq \mathbb{IR}$.
  - When $j = @^{t}_{[a,b]}$, 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: a continuous function on $\mathbb{R}$.
  - Evaluation of x at a point $r : \mathbb{R}$ is given by $@_{[r,r]}x \in \mathbb{R}_{@[r,r]}$
  - We denote this $x^{@}(r)$.

Derivatives of continuous reals

We can define derivatives internally.

- Semantics of $x : \mathbb{R}_\pi$ is: a continuous function on $\mathbb{R}$.
  - Evaluation of x at a point $r : \mathbb{R}$ is given by $@_{[r,r]}x \in \mathbb{R}_{@[r,r]}$
  - We denote this $x^@(r)$.
- We define the derivative more gen'ly for any interval function $x : \bar{\underline{\mathbb{R}}}_\pi$.
  - Result is another interval function $\dot{x} : \bar{\underline{\mathbb{R}}}_\pi$, defined by:
  - $q_1 < \dot{x} < q_2$ iff for all $r_1 < r_2 : \mathbb{R}$,

$$q_1 \ll \frac{x^@(r_2) - x^@(r_1)}{r_2 - r_1} \ll q_2.$$

Derivatives of continuous reals

We can define derivatives internally.

- Semantics of $x : \mathbb{R}_\pi$ is: a continuous function on $\mathbb{R}$.
  - Evaluation of x at a point $r : \mathbb{R}$ is given by $@_{[r,r]}x \in \mathbb{R}_{@[r,r]}$
  - We denote this $x^{@}(r)$.
- We define the derivative more gen'ly for any interval function $x : \overline{\underline{\mathbb{R}}}_\pi$.
  - Result is another interval function $\dot{x} : \overline{\underline{\mathbb{R}}}_\pi$, defined by:
  - $q_1 < \dot{x} < q_2$ 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: a continuous function on $\mathbb{R}$.
  - Evaluation of x at a point $r : \mathbb{R}$ is given by $@_{[r,r]}x \in \mathbb{R}_{@[r,r]}$
  - We denote this $x^{@}(r)$.
- We define the derivative more gen'ly for any interval function $x : \overline{\underline{\mathbb{R}}}_\pi$.
  - Result is another interval function $\dot{x} : \overline{\underline{\mathbb{R}}}_\pi$, defined by:
  - $q_1 < \dot{x} < q_2$ 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.
- Theorem: $\dot{x}$ externally has semantics of derivative of x.

Differential equations

- As a logical expression, derivatives work like anything else.
- Consider a differential equation, like

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

is just a formula in the logic.

Differential equations

- As a logical expression, derivatives work like anything else.
- Consider a differential equation, like

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

  is just a formula in the logic.
- We also define “labeled transition systems” internally...
  - ...given two constant sheaves and two maps $E \rightrightarrows V$.
  - Can more generally define any “hybrid system”.

Outline

Setup of safety problem

Variables to be used, and their types:

$$t : \texttt{Time}. \quad T, P : \mathsf{Cmnd}. \quad a : \mathbb{R}_\pi. \quad \texttt{safe}, \texttt{margin}, \texttt{del}, \texttt{rate} : \mathbb{Q}.$$

What these mean:

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

Behavior contracts

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

Axioms from disparate models of behavior:

- $\theta_1 \coloneqq (\mathtt{margin} > 0) \wedge (a \geq 0)$.

Behavior contracts

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

Axioms from disparate models of behavior:

- $\theta_1 \coloneqq (\mathtt{margin} > 0) \wedge (a \geq 0)$.
- $\theta_2 \coloneqq (a > \mathtt{safe} + \mathtt{margin} \Rightarrow T = \mathtt{level})$.
- $\theta_2' \coloneqq (a < \mathtt{safe} + \mathtt{margin} \Rightarrow T = \mathtt{climb})$.

Behavior contracts

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

Axioms from disparate models of behavior:

- $\theta_1 \coloneqq (\mathtt{margin} > 0) \wedge (a \geq 0)$.
- $\theta_2 \coloneqq (a > \mathtt{safe} + \mathtt{margin} \Rightarrow T = \mathtt{level})$.
- $\theta_2' \coloneqq (a < \mathtt{safe} + \mathtt{margin} \Rightarrow T = \mathtt{climb})$.
- $\theta_3 \coloneqq (P = \mathtt{level} \Rightarrow \dot{a} = 0) \wedge (P = \mathtt{climb} \Rightarrow \dot{a} = \mathtt{rate})$.

Behavior contracts

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

Axioms from disparate models of behavior:

- $\theta_1 \coloneqq (\mathtt{margin} > 0) \wedge (a \geq 0)$.
- $\theta_2 \coloneqq (a > \mathtt{safe} + \mathtt{margin} \Rightarrow T = \mathtt{level})$.
- $\theta_2' \coloneqq (a < \mathtt{safe} + \mathtt{margin} \Rightarrow T = \mathtt{climb})$.
- $\theta_3 \coloneqq (P = \mathtt{level} \Rightarrow \dot{a} = 0) \wedge (P = \mathtt{climb} \Rightarrow \dot{a} = \mathtt{rate})$.
- $\theta_4 \coloneqq \text{is\_delayed}(\mathtt{del}, T, P)$.
    - This is an abbreviation for a longer logical condition.

Behavior contracts

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

Axioms from disparate models of behavior:

- $\theta_1 \coloneqq (\mathtt{margin} > 0) \wedge (a \geq 0)$.
- $\theta_2 \coloneqq (a > \mathtt{safe} + \mathtt{margin} \Rightarrow T = \mathtt{level})$.
- $\theta_2' \coloneqq (a < \mathtt{safe} + \mathtt{margin} \Rightarrow T = \mathtt{climb})$.
- $\theta_3 \coloneqq (P = \mathtt{level} \Rightarrow \dot{a} = 0) \wedge (P = \mathtt{climb} \Rightarrow \dot{a} = \mathtt{rate})$.
- $\theta_4 \coloneqq \text{is\_delayed}(\mathtt{del}, T, P)$.
  - This is an abbreviation for a longer logical condition.

Can prove safe separation

$$\forall (t : \mathtt{Time}). \downarrow_0^t \left(t > \mathtt{del} + \frac{\mathtt{safe}}{\mathtt{rate}} \Rightarrow a \geq \mathtt{safe}\right).$$

Outline

If you're interested in reading more

Two related books:

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

If you're interested in reading more

Two related books:

- *Temporal Type Theory* (Springer Berkhaüser)
    - Freely available: `https://arxiv.org/abs/1710.10258`
    - Technical parts, some friendly parts
- *Seven Sketches in Compositionality* (Cambridge University Press?)
    - Joint with Brendan Fong
    - Freely available: `https://arxiv.org/abs/1803.05316`
    - Chapter 7 is about this material
    - Totally friendly!

If you're interested in reading more

Two related books:

- *Temporal Type Theory* (Springer Berkhaüser)
  - Freely available: `https://arxiv.org/abs/1710.10258`
  - Technical parts, some friendly parts
- *Seven Sketches in Compositionality* (Cambridge University Press?)
  - Joint with Brendan Fong
  - Freely available: `https://arxiv.org/abs/1803.05316`
  - Chapter 7 is about this material
  - Totally friendly!

Questions and comments are welcome. Thanks!