A higher-order temporal logic
for dynamical systems

David I. Spivak*   Patrick Schultz
Christina Vasilakopoulou

Department of Mathematics
Massachusetts Institute of Technology

Outline

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

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.

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]

[1]Traffic 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
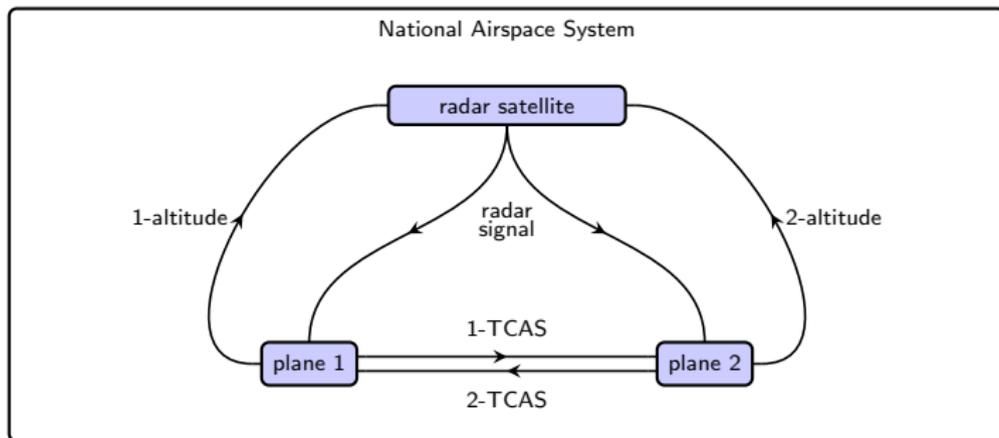
Systems of interacting systems in the NAS
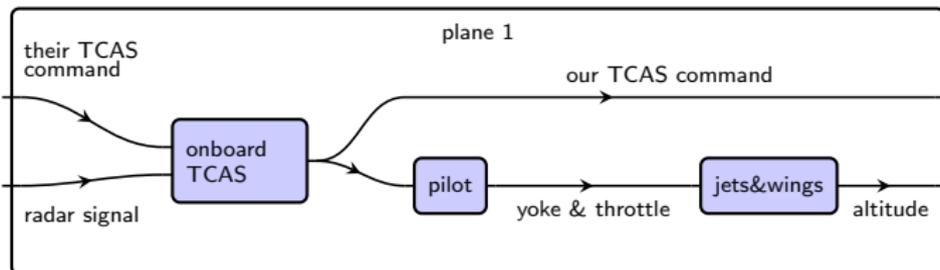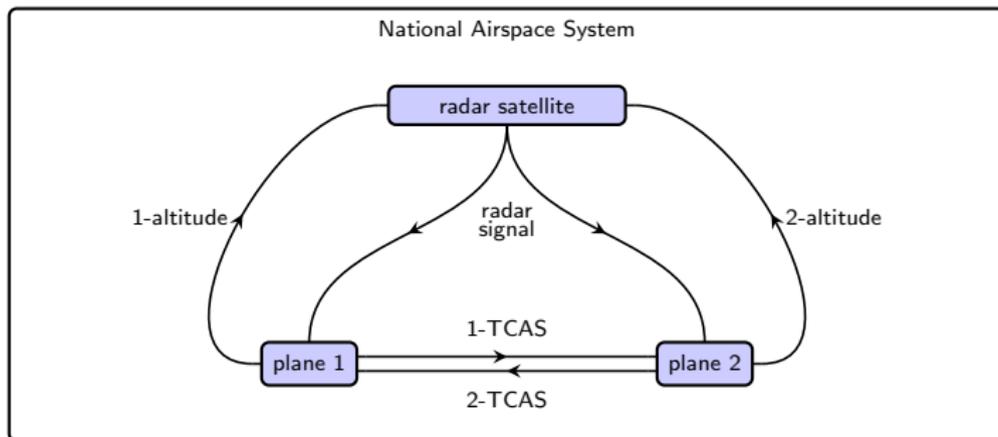
A hypergraph category
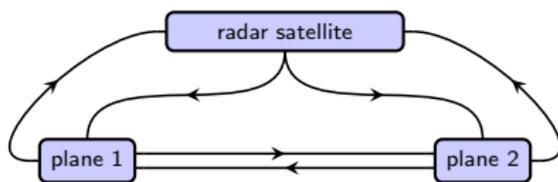
- What are these pictures?
  - Wires with arrows indicate "signal passing".

A hypergraph category

- What are these pictures?
    - Wires with arrows indicate "signal passing".
    - Drop the arrows for "variable sharing" perspective (Willems)
    - Either way, the planes and the radars are *constraints*.
    - "If I know you're close below me, I'll move up".

A hypergraph category

- What are these pictures?
    - Wires with arrows indicate "signal passing".
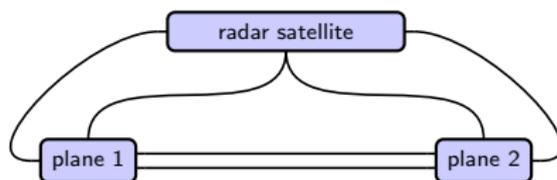   - Drop the arrows for "variable sharing" perspective (Willems)
    - Either way, the planes and the radars are *constraints*.
    - "If I know you're close below me, I'll move up".
- What are these pictures formally?
    - Composition diagrams in a *hypergraph category*.
    - Example of a hypergraph category: relations.
        - where each wire is a set,
        - and each box is a relation $R \subseteq A_1 \times \cdots \times A_n$.

Relations in a topos
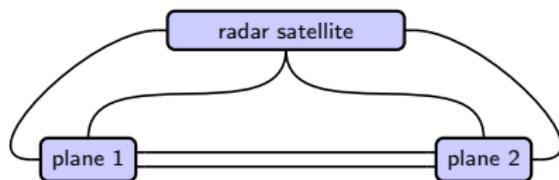
Relations form a hypergraph category *in any topos* $\mathcal{E}$.

Relations in a topos
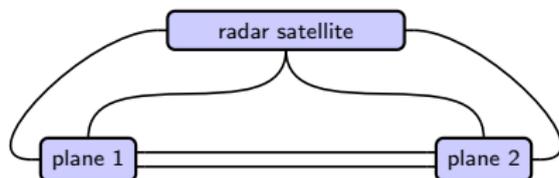
Relations form a hypergraph category *in any topos* $\mathcal{E}$.

- We talked about relations in $\mathcal{E} = \mathbf{Set}$.
- Idea generalizes to arbitrary toposes.
- Every topos $\mathcal{E}$ has a subobject classifier Ω
- Relations on $A = A_1 \times \cdots \times A_n$ are morphisms $A \to \Omega$.

Relations in a topos

Relations form a hypergraph category *in any topos* $\mathcal{E}$.

- We talked about relations in $\mathcal{E} = \textbf{Set}$.
- Idea generalizes to arbitrary toposes.
- Every topos $\mathcal{E}$ has a subobject classifier Ω
- Relations on $A = A_1 \times \cdots \times A_n$ are morphisms $A \to \Omega$.

So... what's the topos for the National Airspace System?

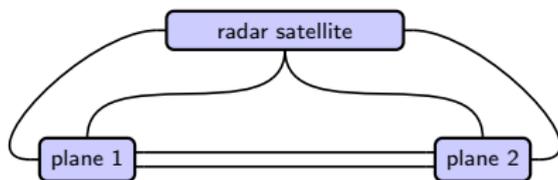- More generally, where do all these behaviors live?

Relations in a topos
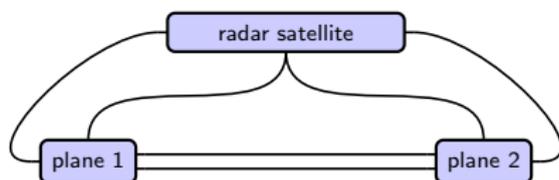
Relations form a hypergraph category *in any topos* $\mathcal{E}$.

- We talked about relations in $\mathcal{E} = \mathbf{Set}$.
- Idea generalizes to arbitrary toposes.
- Every topos $\mathcal{E}$ has a subobject classifier Ω
- Relations on $A = A_1 \times \cdots \times A_n$ are morphisms $A \to \Omega$.

So... what's the topos for the National Airspace System?

- More generally, where do all these behaviors live?
- They live in time.
- Goal: a good topos for studying behaviors (hence time).

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.

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.
- Need a logic in which to prove safety of the combined system.

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.
- Need a logic in which to prove safety of the combined system.

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

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

What is a topos and why?

Toposes—invented by Grothendieck—generalize topological spaces.

- Basic idea:
    - A topos tells you "what can live on a space"...
    - ...rather than telling you "what the space *is*".
    - The space is just the habitat, or "site", where stuff appears.

What is a topos and why?

Toposes—invented by Grothendieck—generalize topological spaces.

- Basic idea:
    - A topos tells you "what can live on a space"...
    - ...rather than telling you "what the space *is*".
    - The space is just the habitat, or "site", where stuff appears.
- Definition: a *topos* is the category of sheaves on a site.
- Two examples: topological spaces and databases.
    - Any topological space defines a site.
    - What lives there: vector fields, scalar fields; "bundles" of stuff.

What is a topos and why?

Toposes—invented by Grothendieck—generalize topological spaces.

- Basic idea:
  - A topos tells you "what can live on a space"...
  - ...rather than telling you "what the space *is*".
  - The space is just the habitat, or "site", where stuff appears.
- Definition: a *topos* is the category of sheaves on a site.
- Two examples: topological spaces and databases.
  - Any topological space defines a site.
  - What lives there: vector fields, scalar fields; "bundles" of stuff.
  - Any database schema S defines a site.
  - What lives there: all S-instances.

What is a topos and why?

Toposes—invented by Grothendieck—generalize topological spaces.

- Basic idea:
    - A topos tells you "what can live on a space"...
    - ...rather than telling you "what the space *is*".
    - The space is just the habitat, or "site", where stuff appears.
- Definition: a *topos* is the category of sheaves on a site.
- Two examples: topological spaces and databases.
    - Any topological space defines a site.
    - What lives there: vector fields, scalar fields; "bundles" of stuff.
    - Any database schema *S* defines a site.
    - What lives there: all *S*-instances.

Question: What's a good site at which *behaviors* live?

First guess: the space $\mathbb{R}$

A first guess: the space $\mathbb{R}$ as the site for behaviors.

First guess: the space $\mathbb{R}$

A first guess: the space $\mathbb{R}$ as the 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: the space $\mathbb{R}$

A first guess: the space $\mathbb{R}$ as the 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 behaviors to subintervals."

First guess: the space $\mathbb{R}$

A first guess: the space $\mathbb{R}$ as the 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 $B(a, b) \rightarrow B(a', b')$
    - "The B-way to restrict behaviors to subintervals."
  - Compatibility:
    - Restriction maps compose: $B(a, b) \rightarrow B(a', b') \rightarrow B(a'', b'')$.

First guess: the space $\mathbb{R}$

A first guess: the space $\mathbb{R}$ as the 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 behaviors to subintervals."
  - Compatibility:
    - Restriction maps compose: $B(a, b) \to B(a', b') \to B(a'', b'')$.
  - Gluing conditions:
    - "Continuity": $B(a, b) = \lim_{a < a' < b' < b} B(a', b')$.
    - "Composition": $B(a, b) = B(a, b') \times_{B(a', b')} B(a', b)$.
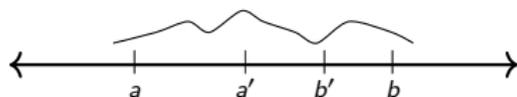
Why $\mathbb{R}$ is not preferable as the site

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

- Want behavior types with non-composable behaviors
    - "Roughly monotonic": $\forall(t_1, t_2). \ t_1 + 5 \leq t_2 \Rightarrow f(t_1) \leq f(t_2)$.
    - "Bounded distance": $\forall(t_1, t_2). -5 < f(t_1) - f(t_2) < 5$.
    - Neither of these have the "composition gluing".

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

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

- Want behavior types with non-composable behaviors
    - "Roughly monotonic": $\forall(t_1, t_2). \, t_1 + 5 \le t_2 \Rightarrow f(t_1) \le f(t_2)$.
    - "Bounded distance": $\forall(t_1, t_2). \, -5 < f(t_1) - f(t_2) < 5$.
    - Neither of these have the "composition gluing".
- Want to compare behavior across different time windows.
    - Example: a delay is "the same behavior at different times."
    - $\mathrm{Shv}(\mathbb{R})$ sees no relation 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.

- Want behavior types with non-composable behaviors
    - "Roughly monotonic": $\forall(t_1, t_2). \ t_1 + 5 \leq t_2 \Rightarrow f(t_1) \leq f(t_2)$.
    - "Bounded distance": $\forall(t_1, t_2). \ -5 < f(t_1) - f(t_2) < 5$.
    - Neither of these have the "composition gluing".
- Want to compare behavior across different time windows.
    - Example: a delay is "the same behavior at different times."
    - $\text{Shv}(\mathbb{R})$ sees no relation between $B(0, 3)$ and $B(2, 5)$.
    - To fix this, replace interval (a, b) by duration $b - a$.
    - "Translation invariance."

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

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

- Want behavior types with non-composable behaviors
    - "Roughly monotonic": $\forall(t_1, t_2).\ t_1 + 5 \leq t_2 \Rightarrow f(t_1) \leq f(t_2)$.
    - "Bounded distance": $\forall(t_1, t_2).\ -5 < f(t_1) - f(t_2) < 5$.
    - Neither of these have the "composition gluing".
- Want to compare behavior across different time windows.
    - Example: a delay is "the same behavior at different times."
    - $\mathrm{Shv}(\mathbb{R})$ sees no relation between $B(0, 3)$ and $B(2, 5)$.
    - To fix this, replace interval (a, b) by duration $b - a$.
    - "Translation invariance."

We'll discard composition gluing and add translation invariance.

The interval domain $\mathbb{IR}$

Discarding composition gluing, we have the site:

- Category: the poset of intervals $(a, b) \subseteq \mathbb{R}$.
- Coverage: $B(a, b) = \lim_{a < a' < b' < b} B(a', b')$.

The interval domain $\mathbb{IR}$

Discarding composition gluing, we have the site:

- Category: the poset of intervals $(a, b) \subseteq \mathbb{R}$.
- Coverage: $B(a, b) = \lim_{a < a' < b' < b} B(a', b')$.

This corresponds to what's called the *interval domain* $\mathbb{IR}$.

- It's a topological space, not Hausdorff, but sober.
- Points: intervals $[d, u]$ (down/up).
- Basis: open intervals (a, b), denoting $\{[d, u] \mid a < d \leq u < b\}$.

The interval domain $\mathbb{IR}$

Discarding composition gluing, we have the site:

- Category: the poset of intervals $(a, b) \subseteq \mathbb{R}$.
- Coverage: $B(a, b) = \lim_{a < a' < b' < b} B(a', b')$.

This corresponds to what's called the *interval domain* $\mathbb{IR}$.

- It's a topological space, not Hausdorff, but sober.
- Points: intervals $[d, u]$ (down/up).
- Basis: open intervals (a, b), denoting $\{[d, u] \mid a < d \leq u < b\}$.

Specialization order on points: $[d, u] \sqsubseteq [d', u']$ means $d \leq d' \leq u' \leq u$.

$\mathbb{IR}$ and the upper half-plane

We'll visualize $\mathbb{IR}$ using the upper half-plane, $H = \{(x, y) \in \mathbb{R}^2 \mid 0 \le y\}$.

Idea: midpoint and radius.... Let's replace variables.

$\mathbb{IR}$ and the upper half-plane

We'll visualize $\mathbb{IR}$ using the upper half-plane, $H = \{(m, r) \in \mathbb{R}^2 \mid 0 \le r\}$.

$\mathbb{IR}$ and the upper half-plane

We'll visualize $\mathbb{IR}$ using the upper half-plane, $H = \{(m, r) \in \mathbb{R}^2 \mid 0 \le r\}$.

- There's a continuous bijection $H \xrightarrow{\cong} \mathbb{IR}$.

$\mathbb{IR}$ and the upper half-plane

We'll visualize $\mathbb{IR}$ using the upper half-plane, $H = \{(m, r) \in \mathbb{R}^2 \mid 0 \le r\}$.

- There's a continuous bijection $H \xrightarrow{\cong} \mathbb{IR}$.
- Map forward: $(m, r) \mapsto [m + r, m - r]$.
- Map backward: $[d, u] \mapsto (\frac{u+d}{2}, \frac{u-d}{2})$.

There's a bijection, but H has more open sets.

Order and opens in $\mathbb{IR}$, from the half-plane perspective

$(m, r) \sqsubseteq (m', r')$ is this sort of "cone" relationship
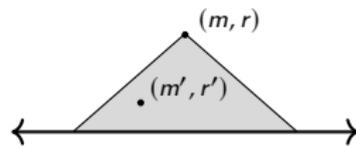
Order and opens in $\mathbb{IR}$, from the half-plane perspective

$(m, r) \sqsubseteq (m', r')$ is this sort of "cone" relationship
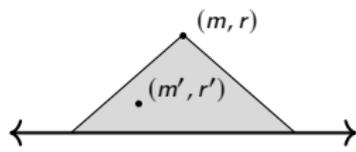
The opens are in bijection with Lipschitz functions $f \colon \mathbb{R} \to \mathbb{R}^+$.

- Here $\mathbb{R}^+ := \{r \in \mathbb{R} \mid r \geq 0\} \cup \{\infty\}$.
- Given such an f, the set of all (m, r) with $r < f(m)$ is open.

Order and opens in $\mathbb{IR}$, from the half-plane perspective

$(m, r) \sqsubseteq (m', r')$ is this sort of "cone" relationship
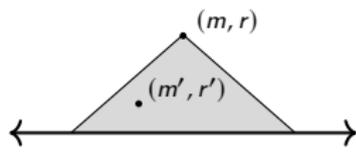
The opens are in bijection with Lipschitz functions $f : \mathbb{R} \to \mathbb{R}^+$.
- Here $\mathbb{R}^+ := \{r \in \mathbb{R} \mid r \geq 0\} \cup \{\infty\}$.
- Given such an f, the set of all (m, r) with $r < f(m)$ is open.

Here's a picture of an open set:

Translation invariance

We want to compare behaviors from different time-windows.

- For example, a delay is "same behavior at different times".
- How to do it?

Translation invariance

We want to compare behaviors from different time-windows.

- For example, a delay is "same behavior at different times".
- How to do it?
    - Consider the translation action $\triangleright \colon \mathbb{R} \times \mathbb{IR} \to \mathbb{IR}$.
        - $(\mathbb{R}, 0, +)$ is a group.
        - It acts on $\mathbb{IR}$ by $r \triangleright [d, u] = [r + d, r + u]$.

Translation invariance

We want to compare behaviors from different time-windows.

- For example, a delay is "same behavior at different times".
- How to do it?
    - Consider the translation action $\triangleright \colon \mathbb{R} \times \mathbb{IR} \to \mathbb{IR}$.
        - $(\mathbb{R}, 0, +)$ is a group.
        - It acts on $\mathbb{IR}$ by $r \triangleright [d, u] = [r + d, r + u]$.
    - Define $\mathbb{IR}_{/\triangleright}$ to be the quotient of $\mathbb{IR}$ by this action.
    - Call $\mathbb{IR}_{/\triangleright}$ the site of *translation-invariant intervals*.

Translation invariance

We want to compare behaviors from different time-windows.

- For example, a delay is "same behavior at different times".
- How to do it?
    - Consider the translation action $\rhd \colon \mathbb{R} \times \mathbb{IR} \to \mathbb{IR}$.
        - $(\mathbb{R}, 0, +)$ is a group.
        - It acts on $\mathbb{IR}$ by $r \rhd [d, u] = [r + d, r + u]$.
    - Define $\mathbb{IR}_{/\rhd}$ to be the quotient of $\mathbb{IR}$ by this action.
    - Call $\mathbb{IR}_{/\rhd}$ the site of *translation-invariant intervals*.
- We'll see that the associated topos has an object Time.
- We can use it to look at behaviors over different time-windows.

Our choice of topos $\mathcal{B}$

Equivalently, $\mathbb{R}_{/\triangleright}$ is the following site:

- Objects $= \{\ell \in \mathbb{R}_{\geq 0}\}$.
- $\text{Hom}(\ell', \ell) = \{\langle r, s \rangle \mid r + \ell' + s = \ell\}$
- Coverage $\{\langle r, s \rangle \colon \ell' \to \ell \mid r > 0, s > 0\}$.
- When $r, s > 0$, write $\ell' \rightsquigarrow \ell$.[2]

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

---

[2] Johnstone-Joyal's notation in "Continuous categories and exponentiable toposes".

Our choice of topos $\mathcal{B}$

Equivalently, $\mathbb{R}_{/\rhd}$ is the following site:

- Objects $= \{\ell \in \mathbb{R}_{\geq 0}\}$.
- $\mathrm{Hom}(\ell', \ell) = \{\langle r, s \rangle \mid r + \ell' + s = \ell\}$
- Coverage $\{\langle r, s \rangle \colon \ell' \to \ell \mid r > 0, s > 0\}$.
- When $r, s > 0$, write $\ell' \rightsquigarrow \ell$.[2]

The topos of behavior types: $\mathcal{B} = \mathrm{Shv}(\mathbb{R}_{/\rhd})$.

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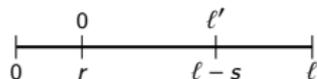
---

[2] Johnstone-Joyal's notation in "Continuous categories and exponentiable toposes".

Our choice of topos $\mathcal{B}$

Equivalently, $\mathbb{R}_{/\triangleright}$ is the following site:

- Objects $= \{\ell \in \mathbb{R}_{\geq 0}\}$.
- $\mathrm{Hom}(\ell', \ell) = \{\langle r, s \rangle \mid r + \ell' + s = \ell\}$
- Coverage $\{\langle r, s \rangle \colon \ell' \to \ell \mid r > 0, s > 0\}$.
- When $r, s > 0$, write $\ell' \rightsquigarrow \ell$.[2]
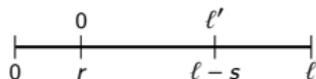
The topos of behavior types: $\mathcal{B} = \mathsf{Shv}(\mathbb{R}_{/\triangleright})$.

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

Example `Time` $\in \mathcal{B}$, the behavior type of a clock:

- `Time`$(\ell) := \{(d, u) \in \mathbb{R}^2 \mid u - d = \ell\}$.
- For $\langle r, s \rangle \colon \ell' \to \ell$ the restriction is $(d, u)\big|_{\langle r, s \rangle} := (d + r, u - s)$.
- The required map is iso.

---

[2] Johnstone-Joyal's notation in "Continuous categories and exponentiable toposes".

Outline

1 Introduction

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

3 Temporal type theory
- Toposes, type theory, and logic
- Type-theoretic presentation
- Modalities and subtoposes
- The derivative

4 Application to the NAS

5 Conclusion

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

Types, terms, and axioms

Type theory is useful, e.g. in computer science.

- It's basically a bunch of language rules.

Types, terms, and axioms

Type theory is useful, e.g. in computer science.

- It's basically a bunch of language rules.
- E.g. simply-typed lambda calculus with sum types and quotient types.
    - Start with atomic types, terms, and predicates.
    - Build new types, terms, and propositions using constructors.
        - Types: $\mathbb{N}$, Prop, products, arrows, sums, quotients.
        - Terms: tupling, projection, lambda abstraction, evaluation, etc.
        - Predicates: $\exists, \forall, \wedge, \vee, \neg, \Rightarrow, \top, \bot$.
    - Add axioms, which are logical statements.

Types, terms, and axioms

Type theory is useful, e.g. in computer science.

- It's basically a bunch of language rules.
- E.g. simply-typed lambda calculus with sum types and quotient types.
    - Start with atomic types, terms, and predicates.
    - Build new types, terms, and propositions using constructors.
        - Types: $\mathbb{N}$, `Prop`, products, arrows, sums, quotients.
        - Terms: tupling, projection, lambda abstraction, evaluation, etc.
        - Predicates: $\exists, \forall, \wedge, \vee, \neg, \Rightarrow, \top, \bot$.
    - Add axioms, which are logical statements.

I thought this was dreadfully boring. Until I witnessed...

The Kripke-Joyal semantics

The Kripke-Joyal semantics is pretty neat.

- Start with atomic types, terms, and axioms from your topos.
- Kripke-Joyal is a machine that turns logic into topos-proofs.

The Kripke-Joyal semantics

The Kripke-Joyal semantics is pretty neat.

- Start with atomic types, terms, and axioms from your topos.
- Kripke-Joyal is a machine that turns logic into topos-proofs.
- Suppose you have any expression in the type theory.
  - It automatically has semantics in your topos.
  - That is, it means something about sheaves X.
  - $\forall(x : X)$ – "for all restriction maps and sections x..."
  - $\exists(x : X)$ – "there is a covering family and a section x in each..."
  - Each connective $\wedge, \vee, \Rightarrow$, means something sheafy.
- Statements and proofs are recursive, tree-like structures.
  - Kripke-Joyal recurses over that structure.
  - At each step, it unwinds the logic into restrictions, covers, sections.
  - It manages all the topos stuff and lets you believe you're in **Set**.

The Kripke-Joyal semantics: doing the heavy lifting.

Dedekind numeric objects

One can define the real numbers in the type theory.

- Follow Dedekind: a real is two subsets of $\mathbb{Q}$.
  - $\mathbb{R} := \{(\delta, \upsilon) : (\mathbb{Q} \to \mathtt{Prop}) \times (\mathbb{Q} \to \mathtt{Prop}) \mid \cdots$

Dedekind numeric objects

One can define the real numbers in the type theory.

- Follow Dedekind: a real is two subsets of $\mathbb{Q}$.
  - $\mathbb{R} := \{(\delta, \upsilon) : (\mathbb{Q} \to \mathtt{Prop}) \times (\mathbb{Q} \to \mathtt{Prop}) \mid \cdots$
  - Bounded: $\exists (q : \mathbb{Q}). \delta q$ and $\exists (q : \mathbb{Q}). \upsilon q$,
  - δ-Rounded: $\forall (q : \mathbb{Q}). \delta q \Leftrightarrow \exists (q' : \mathbb{Q}). (q < q') \wedge \delta q'$,
  - υ-Rounded: $\forall (q : \mathbb{Q}). \upsilon q \Leftrightarrow \exists (q' : \mathbb{Q}). (q' < q) \wedge \upsilon q'$,
  - Disjoint: $\forall (q : \mathbb{Q}). (\delta q \wedge \upsilon q) \Rightarrow \bot$,
  - Located: $\forall (q_1, q_2 : \mathbb{Q}). (q_1 < q_2) \Rightarrow (\delta q_1 \vee \upsilon q_2) \}$.

Dedekind numeric objects

One can define the real numbers in the type theory.

- Follow Dedekind: a real is two subsets of $\mathbb{Q}$.
    - $\mathbb{R} := \{(\delta, \upsilon) : (\mathbb{Q} \to \mathrm{Prop}) \times (\mathbb{Q} \to \mathrm{Prop}) \mid \cdots$
    - Bounded: $\exists(q : \mathbb{Q}). \delta q$ and $\exists(q : \mathbb{Q}). \upsilon q$,
    - δ-Rounded: $\forall(q : \mathbb{Q}). \delta q \Leftrightarrow \exists(q' : \mathbb{Q}). (q < q') \wedge \delta q'$,
    - υ-Rounded: $\forall(q : \mathbb{Q}). \upsilon q \Leftrightarrow \exists(q' : \mathbb{Q}). (q' < q) \wedge \upsilon q'$,
    - Disjoint: $\forall(q : \mathbb{Q}). (\delta q \wedge \upsilon q) \Rightarrow \bot$,
    - Located: $\forall(q_1, q_2 : \mathbb{Q}). (q_1 < q_2) \Rightarrow (\delta q_1 \vee \upsilon q_2) \}$.
- The sheaf $\mathbb{R}$ has a remarkably beautiful semantics.
    - Use Kripke-Joyal to unwind what this is. Find:
    - If $\mathcal{E} = \mathrm{Shv}(T)$ for some topological space T, ...
    - ... $\mathbb{R} =$ sheaf of continuous real-valued functions on T.

Dedekind numeric objects

One can define the real numbers in the type theory.

- Follow Dedekind: a real is two subsets of $\mathbb{Q}$.
  - $\mathbb{R} := \{(\delta, \upsilon) : (\mathbb{Q} \to \mathrm{Prop}) \times (\mathbb{Q} \to \mathrm{Prop}) \mid \cdots$
  - Bounded: $\exists(q : \mathbb{Q}).\, \delta q$ and $\exists(q : \mathbb{Q}).\, \upsilon q$,
  - δ-Rounded: $\forall(q : \mathbb{Q}).\, \delta q \Leftrightarrow \exists(q' : \mathbb{Q}).\, (q < q') \wedge \delta q'$,
  - υ-Rounded: $\forall(q : \mathbb{Q}).\, \upsilon q \Leftrightarrow \exists(q' : \mathbb{Q}).\, (q' < q) \wedge \upsilon q'$,
  - Disjoint: $\forall(q : \mathbb{Q}).\, (\delta q \wedge \upsilon q) \Rightarrow \bot$,
  - Located: $\forall(q_1, q_2 : \mathbb{Q}).\, (q_1 < q_2) \Rightarrow (\delta q_1 \vee \upsilon q_2)\}$.
- The sheaf $\mathbb{R}$ has a remarkably beautiful semantics.
  - Use Kripke-Joyal to unwind what this is. Find:
  - If $\mathcal{E} = \mathrm{Shv}(T)$ for some topological space T, ...
  - ... $\mathbb{R}$ = sheaf of continuous real-valued functions on T.
- Drop various axioms to get other interesting numeric objects.
  - Drop "bounded" and you get unbounded reals.
  - Drop "located" and you get intervals $\mathbb{IR}$, internally.

One new type: Time

One atomic type: Time $\subseteq \mathbb{IR}$.

- Example axiom: Time is an $\mathbb{R}$-torsor:
  - $\forall(r : \mathbb{R})(t : \text{Time}).\, t + r \in \text{Time}$.
  - $\forall(t_1, t_2 : \text{Time}).\, t_1 - t_2 \in \mathbb{R}$.

One new type: `Time`

One atomic type: `Time` $\subseteq \mathbb{IR}$.

- Example axiom: `Time` is an $\mathbb{R}$-torsor:
  - $\forall(r : \mathbb{R})(t : \text{Time}).\, t + r \in \text{Time}$.
  - $\forall(t_1, t_2 : \text{Time}).\, t_1 - t_2 \in \mathbb{R}$.
- With it, we can make temporal logic statements
  - $\forall(t_1, t_2 : \text{Time}).\, (t_1 + 5 \le t_2) \Rightarrow f(t_1) \le f(t_2)$.
  - "The function f is roughly monotonic."
  - Unwind it with Kripke–Joyal, and it has the expected semantics.
- We can also define the real line as a subtopos.

One new type: `Time`

One atomic type: `Time` $\subseteq \mathbb{IR}$.

- Example axiom: `Time` is an $\mathbb{R}$-torsor:
    - $\forall(r : \mathbb{R})(t : \texttt{Time}).\ t + r \in \texttt{Time}$.
    - $\forall(t_1, t_2 : \texttt{Time}).\ t_1 - t_2 \in \mathbb{R}$.
- With it, we can make temporal logic statements
    - $\forall(t_1, t_2 : \texttt{Time}).\ (t_1 + 5 \leq t_2) \Rightarrow f(t_1) \leq f(t_2)$.
    - "The function f is roughly monotonic."
    - Unwind it with Kripke–Joyal, and it has the expected semantics.
- We can also define the real line as a subtopos.

Next up: using logic to define subtoposes.

Modalities in general

We refer to Lawvere-Tierney topologies as *modalities*.[3]

- $j : \mathtt{Prop} \to \mathtt{Prop}$ with $P \Rightarrow jP$, $jjP \Rightarrow jP$, and either of these equivalent conditions:

---

[3]We call them modalities because we're working type-theoretically.

Modalities in general

We refer to Lawvere-Tierney topologies as *modalities*.[3]

- $j : \text{Prop} \to \text{Prop}$ with $P \Rightarrow jP$, $jjP \Rightarrow jP$, and either of these equivalent conditions:
    - $j(P \wedge Q) \Leftrightarrow (jP \wedge jQ)$.
    - $(P \Rightarrow Q) \Rightarrow (jP \Rightarrow jQ)$.

---

[3]We call them modalities because we're working type-theoretically.

Modalities in general

We refer to Lawvere-Tierney topologies as *modalities*.[3]

- $j : \text{Prop} \to \text{Prop}$ with $P \Rightarrow jP$, $jjP \Rightarrow jP$, and either of these equivalent conditions:
    - $j(P \wedge Q) \Leftrightarrow (jP \wedge jQ)$.
    - $(P \Rightarrow Q) \Rightarrow (jP \Rightarrow jQ)$.
- The following are modalities for any $U : \text{Prop}$,
    - open: $\qquad\qquad o_U(P) \coloneqq U \Rightarrow P$,
    - closed: $\qquad\quad\ c_U(P) \coloneqq U \vee P$,
    - quasi-closed: $\quad q_U(P) \coloneqq (P \Rightarrow U) \Rightarrow U$.
- Example: if $U = \bot$ then quasi-closed is double-negation.

---

[3]We call them modalities because we're working type-theoretically.

Modalities in our setting

$j : \texttt{Prop} \rightarrow \texttt{Prop}$ with $P \Rightarrow jP$, $jjP \Rightarrow jP$, $j(P \Rightarrow Q) \Rightarrow (jP \Rightarrow jQ)$.

- Example 1: "t is not not 0": $@_0 P := (P \Rightarrow t \# 0) \Rightarrow t \# 0$.
    - The topos of $@_0^t$ sheaves is an internal copy of **Set**.
    - $\mathbb{R}_{@0}$ is semantically the skyscraper sheaf $\mathbb{R}$ at 0.
- Example 2: "Seeing 0, P": $\downarrow_0 P := (t \# 0) \vee P$.
- Example 3: $\pi P := \forall(t : \texttt{Time}). @_0 P$.

Modalities in our setting

$j : \mathtt{Prop} \to \mathtt{Prop}$ with $P \Rightarrow jP$, $jjP \Rightarrow jP$, $j(P \Rightarrow Q) \Rightarrow (jP \Rightarrow jQ)$.

- Example 1: "t is not not 0": $@_0 P := (P \Rightarrow t \# 0) \Rightarrow t \# 0$.

    - The topos of $@_0^t$ sheaves is an internal copy of **Set**.
    - $\mathbb{R}_{@0}$ is semantically the skyscraper sheaf $\mathbb{R}$ at 0.

- Example 2: "Seeing 0, P": $\downarrow_0 P := (t \# 0) \vee P$.

- Example 3: $\pi P := \forall (t : \mathtt{Time}). @_0 P$.

    - The topos of π-sheaves is an internal copy of $\mathrm{Shv}(\mathbb{R})$.
    - $\mathbb{R}_\pi$ is semantically the usual continuous real-valued functions.

The derivative

Internally define the derivative of $x : \mathbb{R}_\pi$.

- Approximate it with interval-valued functions y:
- Say *y approximates the derivative of x* if, for all $r_1 < r_2$ in $\mathbb{R}$,

$$y \sqsubseteq \frac{x^{@}(r_2) - x^{@}(r_1)}{r_2 - r_1}.$$

- Define $\dot{x}$ to be the limit of such y.

The derivative

Internally define the derivative of $x : \mathbb{R}_\pi$.

- Approximate it with interval-valued functions y:
- Say y *approximates the derivative of* x if, for all $r_1 < r_2$ in $\mathbb{R}$,

$$y \sqsubseteq \frac{x^{@}(r_2) - x^{@}(r_1)}{r_2 - r_1}.$$

- Define $\dot{x}$ to be the limit of such y.

It looks familiar, and it works.

- Internally: linear, $\frac{d}{dt}(t) = 1$, Leibniz rule.
- Externally: it really is the derivative when derivative exists.

Even makes sense when derivative doesn't exist, e.g. absolute value:

$$\frac{d}{dt}|t| = \begin{cases} [-1,-1] & \text{if } t < 0 \\ [-1,1] & \text{if } t = 0 \\ [1,1] & \text{if } t > 0 \end{cases}$$

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 are continuous functions of time.
■ Regardless, it's an equation in the logic.
  ■ Use it with $\top, \bot, \neg, \vee, \wedge, \Rightarrow, \exists, \forall$.
  ■ Can be combined with other properties.

Outline

1. **Introduction**

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

3. **Temporal type theory**

4. **Application to the NAS**
   - A simplified case

5. **Conclusion**

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

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.

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.
- Our 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.
- Our 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:

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

What these mean:

- $t : \mathtt{Time}.$ time-line   (a clock).
- $a : \mathbb{R}_\pi.$ altitude   (continuously changing).
- $T : \mathtt{Cmnd}.$ TCAS command   (occurs at discrete instants).
- $P : \mathtt{Cmnd}.$ 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).

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).
- safe : $\mathbb{Q}$.   safe altitude   (constant).
- margin : $\mathbb{Q}$.   margin-of-error   (constant).
- del : $\mathbb{Q}$.   pilot delay   (constant).
- rate : $\mathbb{Q}$.   maximal ascent rate   (constant).

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

Behavior contracts

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

time-line	(a clock).
altitude	(continuously changing).
TCAS command	(occurs at discrete instants).
pilot's command	(occurs at discrete instants).
safe altitude	(constant).
margin-of-error	(constant).
pilot delay	(constant).
maximal ascent rate	(constant).

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

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).
- safe : $\mathbb{Q}$.   safe altitude   (constant).
- margin : $\mathbb{Q}$.   margin-of-error   (constant).
- del : $\mathbb{Q}$.   pilot delay   (constant).
- rate : $\mathbb{Q}$.   maximal ascent rate   (constant).

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

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).
- safe : $\mathbb{Q}$.   safe altitude   (constant).
- margin : $\mathbb{Q}$.   margin-of-error   (constant).
- del : $\mathbb{Q}$.   pilot delay   (constant).
- rate : $\mathbb{Q}$.   maximal ascent rate   (constant).

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

θ_4 is an abbrevation for a longer logical condition.

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).
- safe : $\mathbb{Q}$.   safe altitude   (constant).
- margin : $\mathbb{Q}$.   margin-of-error   (constant).
- del : $\mathbb{Q}$.   pilot delay   (constant).
- rate : $\mathbb{Q}$.   maximal ascent rate   (constant).

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

θ_4 is an abbrevation for a longer logical condition.

- Can prove safe separation
$$\forall(t : \mathrm{Time}). \downarrow_0 (t > \mathtt{del} + \frac{\mathtt{safe}}{\mathtt{rate}} \ \Rightarrow \ a \geq \mathtt{safe}).$$

Outline

1 **Introduction**

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

3 **Temporal type theory**

4 **Application to the NAS**

5 **Conclusion**
- Summary

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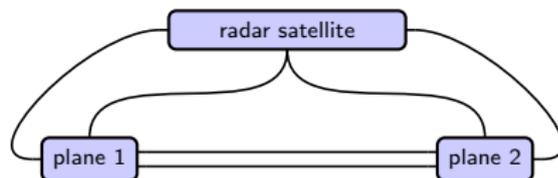
Summary

- Idea: topos theory for integrating systems.
- Systems characterized by their possible behaviors.
    - $\mathcal{B} = \mathsf{Shv}(\mathbb{IR}_{/\triangleright})$: topos of behavior types.
    - $X \in \mathcal{B}$. $X(\ell)=$ "possible behaviors of length-ℓ."

Summary

- Idea: topos theory for integrating systems.
- Systems characterized by their possible behaviors.
    - $\mathcal{B} = \mathsf{Shv}(\mathbb{IR}_{/\triangleright})$: topos of behavior types.
    - $X \in \mathcal{B}$. $X(\ell) =$ "possible behaviors of length-ℓ."

- Integrate systems in a hypergraph category of relations.
    - Each component X has an interface, say $A_1, \ldots, A_n$.
    - Characterize by its property $X : A_1 \times \cdots \times A_n \to \mathtt{Prop}$
    - Differential equations, discrete automata, delays, are examples.

Summary

- Idea: topos theory for integrating systems.
- Systems characterized by their possible behaviors.
    - $\mathcal{B} = \mathsf{Shv}(\mathbb{IR}_{/\rhd})$: topos of behavior types.
    - $X \in \mathcal{B}$. $X(\ell)=$ "possible behaviors of length-ℓ."
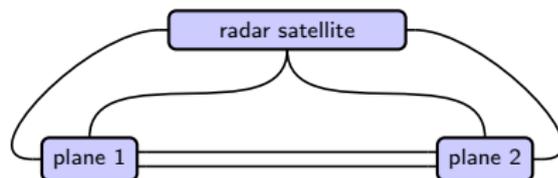
- Integrate systems in a hypergraph category of relations.
    - Each component X has an interface, say $A_1, \ldots, A_n$.
    - Characterize by its property $X : A_1 \times \cdots \times A_n \to \mathtt{Prop}$
    - Differential equations, discrete automata, delays, are examples.
- A new *temporal type theory* with sheaf semantics.

Questions and comments are welcome. Thanks!