

# Sheaf semantics of termination-insensitive noninterference

---

Jonathan Sterling (j.w.w. Robert Harper)

Aarhus University

MURI 2022 Team Meeting

Let  $\phi$  be a proposition in a topos  $\mathbf{X}$ . Then  $\phi$  determines two complementary open/closed subtopoi  $\mathbf{U}, \mathbf{K} \subseteq \mathbf{X}$  via the following Lawvere–Tierney local operators:

$$j_{\mathbf{U}}\psi = \phi \Rightarrow \psi$$

$$j_{\mathbf{K}}\psi = \phi \vee \psi$$

Rijke, Shulman, and Spitters explained how to adapt open and closed modalities to (homotopy) type theory.

1. The **open modality**  $\phi \Rightarrow E$  projects the part of  $E$  that “thinks that”  $\phi$  is true.
2. The **closed modality**  $\phi \bullet E = \phi \sqcup_{\phi \times A} E$  projects the part of  $E$  that “thinks that”  $\phi$  is not true.

Today I will talk about an application to **types for security**.

Computer programs frequently must deal with **sensitive data**.

- your passwords
- your browser history
- your bank account number

The goal of **information flow control** is to provide tools to control the leakage of such data through program outputs.

Measured by **noninterference**: what kind of outputs can depend on what kinds of inputs?

**Our contribution**: a new denotational semantics for information flow control based on **open and closed modalities**.

S., Harper. **Sheaf semantics of termination-insensitive noninterference**. In FSCD 2022.

Noninterference via closed modalities

---

# presheaves on a security (semi)lattice

We start with a meet semilattice  $\mathbb{P}$  to be thought of as the collection of **security clearances**. For instance, we could have:

$$\mathbb{P} = \{\text{low} \leq \text{med} \leq \text{high} \leq \top\}$$

The *presheaf topos*  $\mathbf{P} = \hat{\mathbb{P}}$  is an ideal setting to develop a synthetic theory of security and redaction.

1. An open  $\phi \in \mathcal{O}_{\mathbf{P}} = [\mathbb{P}^{\text{op}}, \Omega]$  is a formal join of security clearances, which we may refer to as a **security policy**.
2. A (pre)sheaf  $A \in \mathcal{S}_{\mathbf{P}} = [\mathbb{P}^{\text{op}}, \mathbf{Set}]$  then has **extent** over each security policy  $\phi \in \mathcal{O}_{\mathbf{P}}$ , *i.e.* we may restrict  $A$  to  $A|_{\phi} = \phi \times A \in \mathcal{S}_{\mathbf{P}} \downarrow \phi$ .

$A|_{\phi}$  is the part of  $A$  that is visible under the policy  $\phi$ .

In particular,  $A|_{\text{med}} \in \mathcal{S}_{\mathbf{P}} \downarrow \text{med}$  is the part of  $A$  that is visible to **medium**- and **low**-security observers.

## open and closed subtopos

For each security policy  $\phi \in \mathcal{O}_{\mathbf{P}}$ , we have a pair of complementary open and closed subtopoi:

1. The **open** subtopos  $\mathbf{U}_{\phi} \subseteq \mathbf{P}$  is defined by setting  $\mathcal{S}_{\mathbf{U}_{\phi}}$  to be the full subcategory of  $\mathcal{S}_{\mathbf{P}}$  spanned by sheaves  $A$  such that  $A \rightarrow A^{\phi}$  is an isomorphism, *i.e.* the slice  $\mathcal{S}_{\mathbf{P}} \downarrow \phi$ .
2. The **closed** subtopos  $\mathbf{K}_{\phi} \subseteq \mathbf{P}$  is defined by setting  $\mathcal{S}_{\mathbf{K}_{\phi}}$  to be the full subcategory of  $\mathcal{S}_{\mathbf{P}}$  spanned by sheaves  $A$  such that  $A \times \phi \rightarrow \phi$  is an isomorphism.

We will visualize the modal operators corresponding to these subtopoi and their application to security.

# a topo-logical viewpoint on redaction

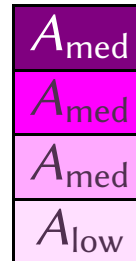
We may visualize an object  $A \in \mathcal{S}_P$  as a “pill” with components corresponding to what is visible at each security level.



Restricting into  $\mathcal{S}_P \downarrow_{med}$  we have a truncated “pill”:



Restriction was the *inverse image* of the open immersion  $\mathbf{P}_{med} \hookrightarrow \mathbf{P}$ . The *direct image* extends our truncated “pill” as follows:

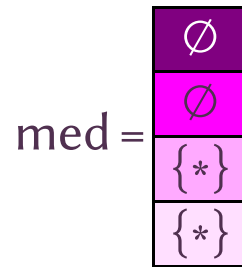


Thus all high-security data is redacted and replaced with medium security data.

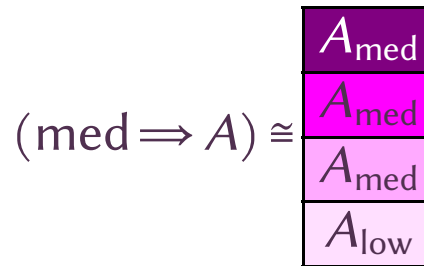


# the open modality as redactor

The round-trip  $\mathcal{S}_P \rightarrow (\mathcal{S}_P \downarrow \text{med}) = \mathcal{S}_{U_{\text{med}}} \hookrightarrow \mathcal{S}_P$  is the **open modality** for the (representable) proposition  $\text{med} \in \mathcal{O}_P$  depicted below:



Indeed, the following is not too hard to compute:

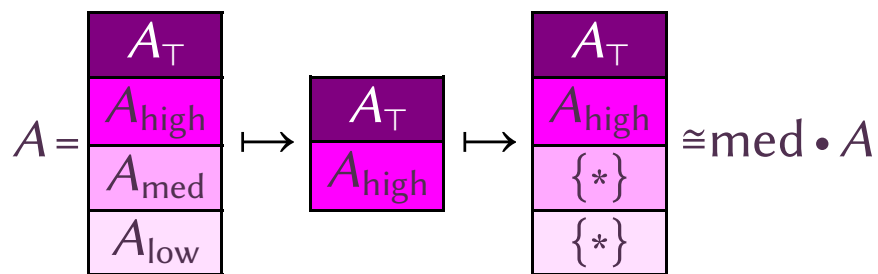


The open modality thus purges higher-security data.

## sealing and closed subspace

The **closed complement**  $\mathbf{K}_{\text{med}}$  to  $\mathbf{U}_{\text{med}}$  is what parameterizes “high security (pre)sheaves”, *i.e.* objects that **only** have extent visible to high and top security observers.

The closure operator corresponding to  $\mathbf{K}_{\text{med}} \subseteq \mathbf{P}$  causes a sheaf  $A \in \mathcal{S}_{\mathbf{P}}$  to appear to contract to a point as far as medium and low security observers are concerned:



This is indeed the closed modality  $\text{med} \cdot A = \text{med} \sqcup_{\text{med} \times A} A$ .

**Here's the application to security.** Suppose we want a type of integers that cannot leak to medium- and low-security clients.

1. We **seal** the type  $\mathbb{Z}$  under the closed modality for  $\text{med} \in \mathcal{O}_p$ , *i.e.* we will use  $\text{med} \bullet \mathbb{Z}$ .
2. Using the universal property of the closed modality, we can always unseal  $\text{med} \bullet \mathbb{Z}$  for consumption by higher security clients, *i.e.* types  $C$  that are contractible within  $\text{med}$ , *i.e.*  $\text{med}$ -connected or  $(\text{med} \bullet -)$ -modal types:

$$(\text{med} \bullet \mathbb{Z} \rightarrow C) \cong (\mathbb{Z} \rightarrow C)$$

**Theorem 1.** *Let  $f : \text{med} \bullet A \rightarrow 2$  be any function; then  $f$  is constant.*

**Proof.** The type  $2$  is *constant*, i.e. we have  $2 =$

{0, 1}
{0, 1}
{0, 1}
{0, 1}

Thus  $2$  is in particular  $(\text{med} \Rightarrow -)$ -modal and so we have:

$$\begin{aligned}
 (\text{med} \bullet A \rightarrow 2) &\cong (\text{med} \bullet A \rightarrow \text{med} \Rightarrow 2) \\
 &\cong \text{med} \Rightarrow (\text{med} \bullet A \rightarrow 2) \\
 &\cong \text{med} \Rightarrow 2 \\
 &\cong 2
 \end{aligned}$$

So we are done.

□

## Partial noninterference via synthetic domain theory

---

## partiality via dominances

In the field of **programming languages** we are mainly interested in languages that support **partial functions** and **general recursion**.

In semantics, partiality means that we have a **dominance**  $\top : 1 \multimap \Sigma$ , *i.e.* a classifier for a collection of monomorphisms that will serve as the supports of partial functions.

The **partial map classifier** is the partial product of  $\top : 1 \multimap \Sigma$ , *i.e.*

$$A_{\perp} = \sum_{\phi : \Sigma} \phi \Rightarrow A$$

A partial function  $C \rightarrow A_{\perp}$  is determined by a total function  $U \rightarrow A$  defined on a  $\Sigma$ -subobject  $U \subseteq C$ .

With partiality, we can consider two kinds of noninterference:

1. **Total noninterference** means that any function  $f : \text{med} \cdot A \rightarrow 2_{\perp}$  is constant. (*a.k.a.* “termination-sensitive noninterference”)
2. **Partial noninterference** means that any function  $f : \text{med} \cdot A \rightarrow 2$  is constant. (*a.k.a.* “termination-insensitive noninterference”)

From partial noninterference we conclude:

$$\forall x, y : \text{med} \cdot A. \quad f x \downarrow \wedge f y \downarrow \rightarrow f x = f y$$

Partial noninterference has been difficult to model satisfactorily in the past (*cf.* [Abadi \*et al.\*](#)). But follows immediately from standard **domain theoretic semantics** if we take **P** as our base topos.

**Synthetic domain theory** (Hyland) is to classical domain theory as synthetic differential geometry is to the theory of manifolds. Take a topos  $\mathbf{D}$  equipped with a dominance  $\top : 1 \multimap \Sigma$ ; the dominance is a **dualizing object** that associates to each object  $X$  a topology  $\Sigma^X$ .

We define a **predomain** to be an object  $X$  of  $\mathcal{S}_{\mathbf{D}}$  satisfying a certain orthogonality condition; many possible conditions, but the weakest one that can possibly work is **well-completeness** (Longley):

Let  $\omega_{\perp} \rightarrow \omega$  be the initial algebra for the endofunctor  $X \mapsto X_{\perp}$  and let  $\bar{\omega} \rightarrow \bar{\omega}_{\perp}$  be the final coalgebra; let  $\omega \multimap \bar{\omega}$  be the canonical inclusion.

**Definition 2.** (Fiore, Plotkin) *An object  $X$  is a **predomain** when it is internally orthogonal to any pullback of  $\omega \multimap \bar{\omega}$  along a  $\Sigma$ -monomorphism  $U \multimap \bar{\omega}$ .*

Orthogonality condition = closure under suprema of  $\omega$ -chains.



## synthetic domain theory over a base topos

Two class of model of SDT have emerged: realizability models and sheaf models. We will focus on sheaf models.

The recipe of **Fiore and Plotkin** is to take sheaves on a small category of ordinary domains (e.g.  $\omega$ -cpos, &c.). Fiore and Plotkin construct Grothendieck topos models of SDT over **Set**, but this recipe works over any base topos.

We construct a model of SDT over  $\mathcal{S}_{\mathbf{P}}$ , i.e. a geometric morphism  $\delta: \mathbf{D} \rightarrow \mathbf{P}$  such that  $\Sigma = \delta^* \Omega_{\mathbf{P}}$ .

The resulting notion of partial map includes not only convergence and divergence, but also divergence *above a certain security level*. There are computations that appear to converge for low-security clients, but can be seen to diverge by high-security clients.

## declassification in the partial map classifier

Let  $A$  be modal for the closed modality  $(\text{med} \bullet -)$ , *i.e.* suppose we have an algebra  $\alpha: \text{med} \bullet A \rightarrow A$ . Then we may define a function

$$\text{dcls}: \text{med} \bullet A_{\perp} \rightarrow A_{\perp}$$

that “unseals” or “declassifies” a partial computation of type  $A$ .

$$\begin{array}{ccc} \text{med} \bullet A & \xrightarrow{\alpha} & A \\ \text{med} \bullet \eta \downarrow & (\text{cart.}) & \downarrow \eta \\ \text{med} \bullet A_{\perp} & \xrightarrow{\text{dcls}} & A_{\perp} \end{array}$$

The subobject  $\text{med} \bullet A \twoheadrightarrow \text{med} \bullet A_{\perp}$  lies in  $\Sigma$  because  $\Sigma$  is closed under the closed modality  $(\text{med} \bullet -)$ : a form of **parallel computation!**

# computational adequacy via synthetic Tait computability

We have defined a denotational semantics in synthetic domain theory for a programming language with modalities for security.

What is the relationship between equality of programs (the equational theory) and equality of their denotations?

**Plotkin's computational adequacy** lemma states that for base types (e.g. booleans) we have  $\vdash e_1 \equiv e_2 : \text{bool}$  if and only if  $\llbracket e_1 \rrbracket = \llbracket e_2 \rrbracket$ .

We prove such a lemma for our language using **synthetic Tait computability**, an axiomatization of the internal language of Artin gluings.

## gluing for computational adequacy, geometrically

1. Let  $\mathbf{T}$  be the classifying topos of our programming language viewed as a lex theory, *i.e.* presheaves on its syntactic category  $\mathbb{T}$ . This is a  $\mathbf{P}$ -topos, as we have a lex functor  $\mathbb{P} \rightarrow \mathbb{T}$  sending each security level to its syntactic counterpart.
2. Let  $\mathbf{D}$  be the  $\mathbf{P}$ -topos model of synthetic domain theory in which we constructed our denotational semantics.
3. Then take the (relative) scone of  $\mathbf{T} + \mathbf{D}$  in the category of bounded  $\mathbf{P}$ -topoi, *i.e.* the following co-comma object  $\mathbf{GTop}$ :

$$\begin{array}{ccc} \mathbf{T} + \mathbf{D} & \xrightarrow{\quad} & \mathbf{P} \\ \downarrow & & \downarrow \perp \\ \mathbf{T} + \mathbf{D} & \xrightarrow[\eta]{} & (\mathbf{T} + \mathbf{D})_{\perp} \end{array}$$

Extend the internal language of a topos with:

1. disjoint propositions  $\Phi_{\text{syn}} \wedge \Phi_{\text{sem}} = \perp$  and define  $\Phi = \Phi_{\text{syn}} \vee \Phi_{\text{sem}}$ ;
2. a **generic** model  $\llbracket - \rrbracket_{\text{syn}}$  of  $\mathbb{T}$  in the slice over  $\Phi_{\text{syn}}$ ;
3. the axioms of  $\mathbb{P}$ -indexed SDT in the slice over  $\Phi_{\text{sem}}$ ;
4. such that for each  $l \in \mathbb{P}$  we have  $\llbracket l \rrbracket_{\text{sem}} \leq \Phi \cdot \llbracket l \rrbracket_{\text{syn}}$ .

Under these axioms, we may construct a **synthetic logical relation** between the generic model and the denotational model that establishes computational adequacy.

**Theorem 3.** *If  $\llbracket \vdash e : \text{bool}_{\perp} \rrbracket = \eta b$  then there exists  $\vdash v : \text{bool}$  such that  $\vdash e \equiv \text{ret}(v) : \text{bool}$  and  $\llbracket \vdash v : \text{bool} \rrbracket = b$ .*

**Corollary 4.** *Partial noninterference holds in the equational theory  $\mathbb{T}$ .*

## towards HIGHER synthetic domain theory?

The results of [Schreiber](#), [Shulman](#), [Cherubini](#), &c. suggest that the [Fiore–Plotkin](#) approach to synthetic domain theory based on **sheaves** and well-completeness should extend directly to  $\infty$ -topoi.

The work of [Awodey](#), [Frey](#), [Speight](#), [Swan](#), [Uemura](#), &c. toward **realizability**  $\infty$ -**topoi** are promising as a direction to generalize the [Hyland–Phoa–Taylor](#) approach to synthetic domain theory based on repleteness.

A step toward recursive programming with higher-dimensional spaces? **Help me do it!**