# Modalities, Cohesion, and Information Flow

Alex Kavvos

Department of Mathematics and Computer Science, Wesleyan University

46th ACM SIGPLAN Symposium on Principles of Programming Languages, 18 Jan 2019

# Language-based Information Flow Control

- General idea:
  - **types** include annotations on the **classification/sensitivity** of data
  - programs should type-check iff there is no **unsafe information flow** (e.g. from TOP SECRET to UNCLASSIFIED)
- Modalities = unary operations on types. $\mathrm{T}(\mathrm{A}) \quad \Box A \quad \blacklozenge A \quad ||A||$
- Modalities can be used to **control information flow**. One can copy techniques from the **proof theory of modal logic**.
- The hard part is proving **noninterference**:

*[...] High-security data does not "interfere" with the calculation of low-security outputs [...]*

# Modalities for Information Flow: an example

- An example: for each type $A$, a type $\blacklozenge A$ ⟵ **"high security A"**
- Can always get a $\blacklozenge A$ : $\dfrac{\Gamma \vdash M : A}{\Gamma \vdash [M] : \blacklozenge A}$
- **I can use a high-security value when computing another high-security value:**

$$\frac{\Gamma \vdash M : \blacklozenge A \quad \Gamma, x : A \vdash N : \blacklozenge C}{\Gamma \vdash \text{let x} = M \text{ in } N : \blacklozenge C}$$

- Reduction: $\text{let x} = [M] \text{ in } N \to N[M/x]$
- Noninterference:

a.k.a.
"Moggi's monadic metalanguage"

> If $x : \blacklozenge A \vdash E : \text{Bool}$ and $\vdash M, N : \blacklozenge A$ then
> $E[M/x]$ and $E[N/x]$ compute the same boolean value.

**How can we go about proving this?**

# Proving noninterference

- This talk: using **category theory** to prove noninterference.
- A more principled attempt at a "theory of information flow."
- Main claim: one can use basic **axiomatic cohesion** to reason about information flow, and prove noninterference results.
- **Axiomatic cohesion**: a theory developed by F. William Lawvere.
  — an axiomatic description of **geometric/topological spaces**.

**CRIB**

U(X) = points of space X (forget cohesion)

Δ(S) = discrete space on S (minimum cohesion)

∇(S) = codiscrete space on S (maximum cohesion)

C(X) = connected components of X

# Cohesion

**Spaces (types)** **(= points + cohesion)**

$C \dashv \Delta \dashv U \dashv \nabla$

"**X** redacted" $\blacklozenge X = \nabla(UX)$

"**X** declassified" $\Box X = \Delta(UX)$

$\int X = \Delta(CX)$

"shape of **X**", or "**X** as viewed by a low security user"

$\int \dashv \Box \dashv \blacklozenge$

**Sets** **(= points)**

| $\mathbb{B}$ | $\Delta(\mathbb{B})$ | $\nabla(\mathbb{B})$ | $C(\Delta(\mathbb{B}))$ | $C(\nabla(\mathbb{B}))$ |
|---|---|---|---|---|
| `tt` `ff` | `tt` `ff` | `tt`—`ff` | `{tt}` `{ff}` | `{tt, ff}` |

# Cohesion

**CRIB**

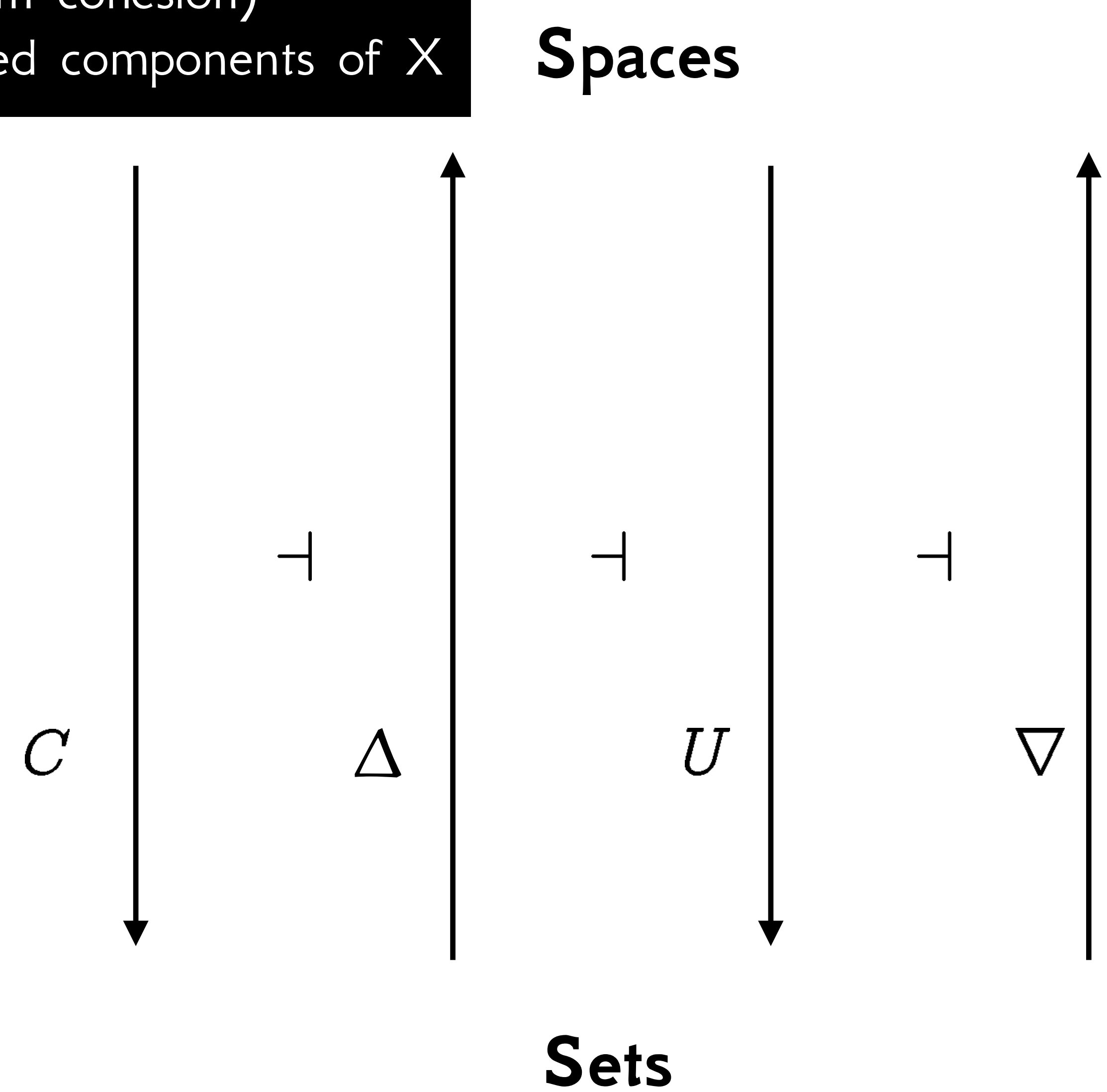
U(X) = points of space X (forget cohesion)

Δ(S) = discrete space on S (minimum cohesion)

∇(S) = codiscrete space on S (maximum cohesion)

C(X) = connected components of X

CLAIM: This is all one needs to reason about information flow.




**Axiom of CONTRACTIBLE CODISCRETENESS:**

$$\forall S.\ |C(\nabla S)| \leq 1$$

(For category theorists: the canonical $C(\nabla S) \xrightarrow{!} \mathbf{1}$ is a monic arrow.)

**Theorem**: every $f : \blacklozenge X \to \Delta S$ is (maybe) a point of S

**Proof**: very simple—three lines of category theory

| $\mathbb{B}$ | $\nabla(\mathbb{B})$ | $C(\nabla(\mathbb{B}))$ |
|---|---|---|
| `tt` `ff` | `tt`—`ff` | {`tt`, `ff`} |

**in the codiscrete space ∇(S) on S everything is "stuck together" ⇒ there is ≤ 1 connected component**

**CRIB**

U(X) = points of space X (forget cohesion)
Δ(S) = discrete space on S (minimum cohesion)
∇(S) = codiscrete space on S (maximum cohesion)
C(X) = connected components of X

# Classified sets

**Set of classifications/labels:** $\ell \in \mathcal{L}$

**Classified set:** $X = (|X|, (R_\ell \subseteq |X| \times |X|)_{\ell \in \mathcal{L}})$

must be **reflexive**

**Cont. function:** $f : X \to Y$ **s.t.** $\forall \ell.\ a R_\ell b \Rightarrow f(a) R_\ell f(b)$

**"f is continuous when it maps inputs indistinguishable at $\ell \in \mathcal{L}$ to outputs indistinguishable at $\ell \in \mathcal{L}$ "**

$$X \xrightarrow{C} \text{(equivalence classes)} \quad \dashv \quad (S, (\{(s,s) \mid s \in S\})_{\ell \in \mathcal{L}}) \xleftarrow{\Delta} S \quad \dashv \quad X \xrightarrow{U} |X| \quad \dashv \quad (S, (S \times S)_{\ell \in \mathcal{L}}) \xleftarrow{\nabla} S$$

It is a model of functional programming languages

It is a model of information flow

**Theorem**: the category of classified sets is **cartesian closed** and **cohesive over Sets**, and it satisfies **contractible codiscreteness.**

# Cohesion and non-interference

- Recall what we were trying to prove:

$$\text{If } \; x : \blacklozenge A \vdash E : \mathsf{Bool} \; \text{ and } \; \vdash M, N : \blacklozenge A \; \text{ then}$$
$$E[M/x] \text{ and } E[N/x] \text{ compute the same boolean value.}$$

- There is a way to map every term to a continuous function between classified sets—a **categorical semantics**:

$$x : \blacklozenge A \vdash E : \mathsf{Bool} \qquad \longmapsto \qquad [\![E]\!] : \blacklozenge [\![A]\!] \to \Delta \mathbb{B}$$

- By the Theorem, this corresponds to an element of $\mathbb{B}$
  So it is essentially a constant function!

- Use Adequacy (holds for strongly normalising languages) to lift to the language

# Cohesion and non-interference

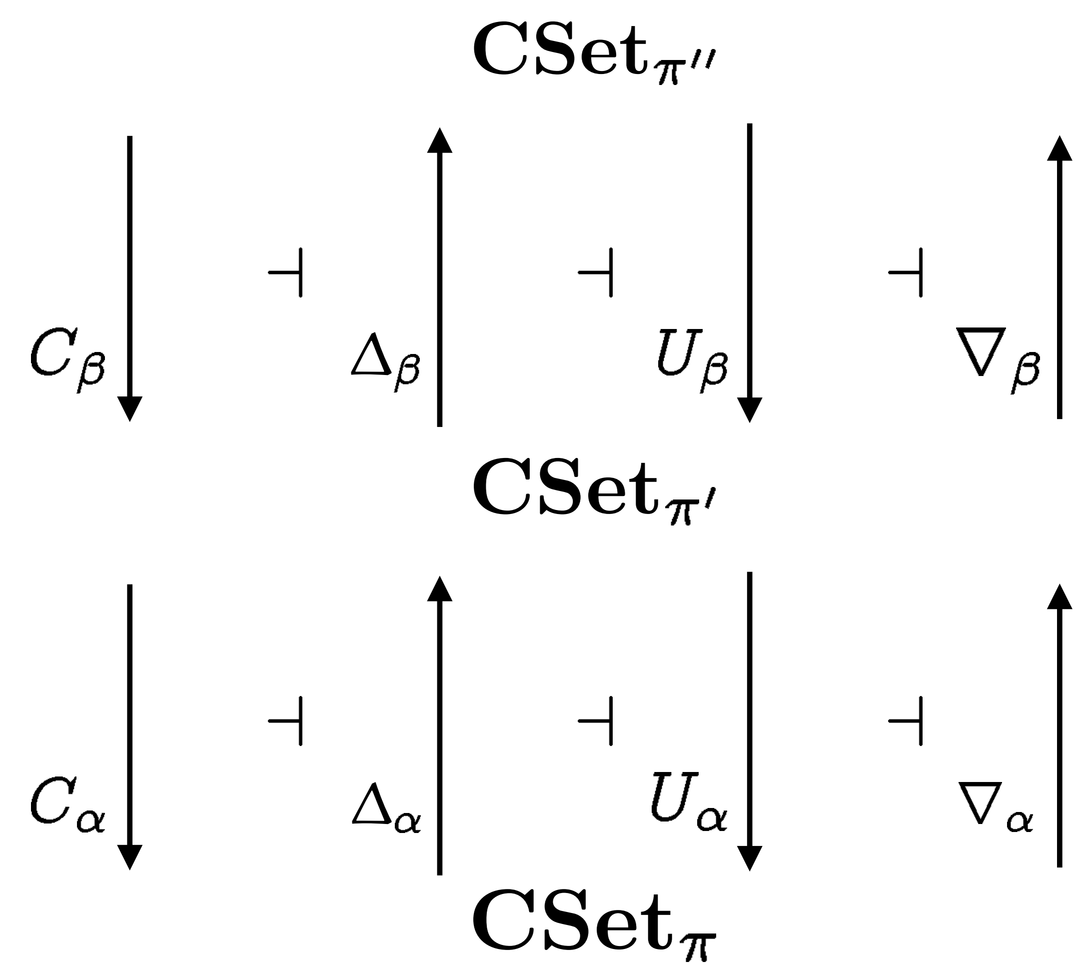
- This approach can be leveraged to prove noninterference for multiple type theories for secure information flow:
  - Moggi's monadic metalanguage [Moggi 1991]
  - Davies-Pfenning calculus (S4 modality) [D&Pf 2001]
  - Dependency Core Calculus [Abadi et al. 1999]
  - Sealing Calculus [Shikuma & Igarashi 2008]

  (A little bit of care is required here w.r.t. adequacy) — applies to the Davies-Pfenning calculus and the Dependency Core Calculus
- The last two are **multi-modal** type theories.

# Cohesion and multi-modal type theories for information flow

Writing $\mathbf{CSet}_\pi$ for the category of classified sets over $\pi \subseteq \mathcal{L}$

and $\begin{array}{l} \alpha : \pi \subseteq \pi' \\ \beta : \pi' \subseteq \pi'' \end{array}$ for the unique morphisms in $\mathcal{P}(\mathcal{L})$ we have the two cohesive situations on the right.

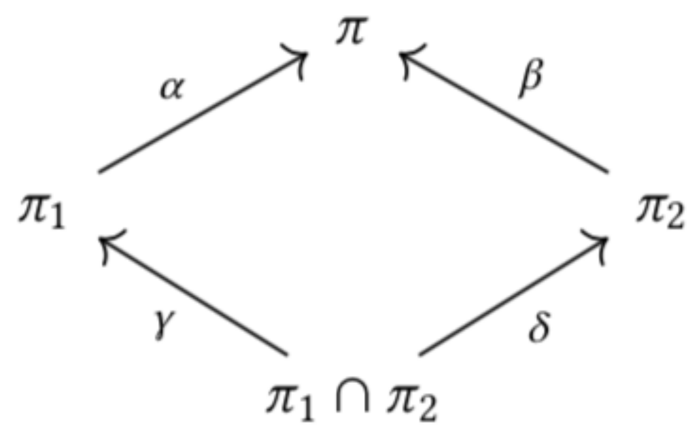



It's a functor

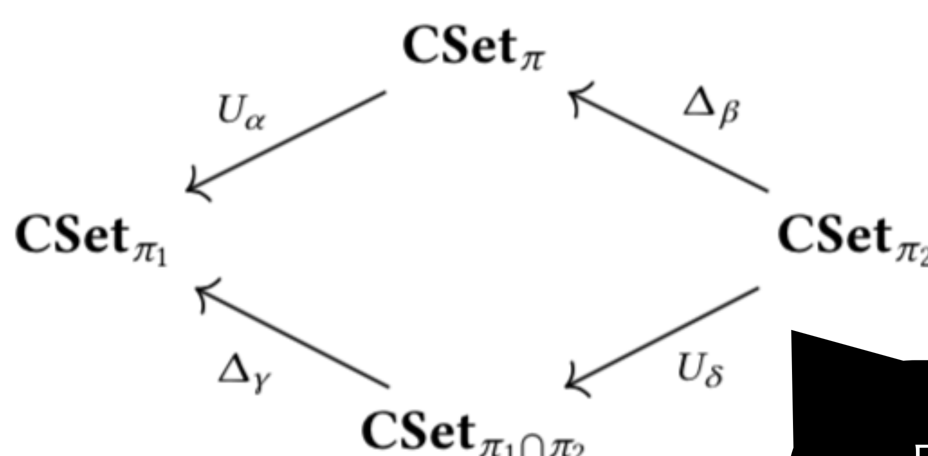
$$\mathcal{P}(\mathcal{L})^{\mathrm{op}} \longrightarrow \mathbf{Coh}$$

**Theorem**: the category of classified sets over $\mathcal{L} \cup \pi$ is **cohesive** over the category of classified sets over $\mathcal{L}$ and satisfies **contractible codiscreteness**.

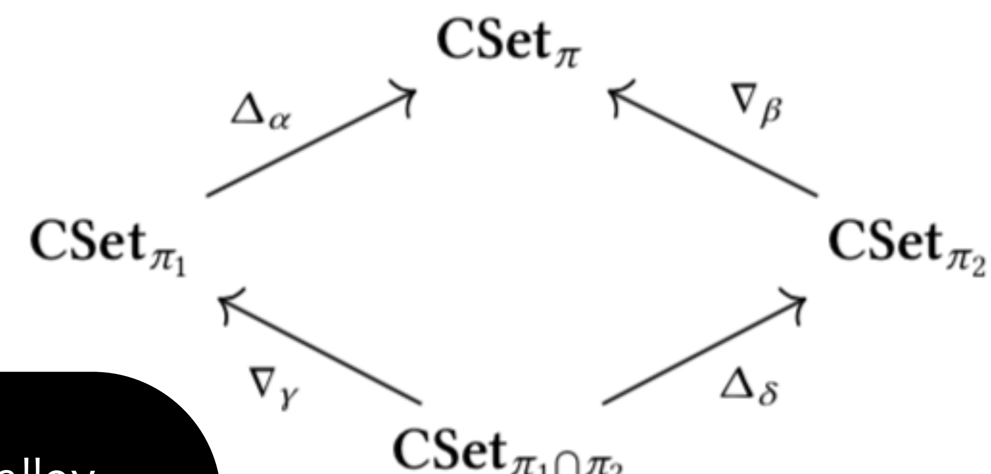
# Three fundamental equations

✤ Given  (a pullback) we want:



**(1)** 



**(3)** 



Beck-Chevalley
(thanks to D. Spivak)

**(2)** same as (1) but for $\nabla$

**Observation**: These suffice to prove all the laws I have needed so far.

# The laws for $\int \dashv \square \dashv \blacklozenge$

PROPOSITION 21.

(1) *If* $\pi \cap \pi' = \emptyset$, *then* $\square_\pi \square_{\pi'} = \square_{\pi \cup \pi'}$.

(2) *If* $\pi \cap \pi' = \emptyset$, *then* $\blacklozenge_\pi \blacklozenge_{\pi'} = \blacklozenge_{\pi \cup \pi'}$.

(3) $\square_\pi \square_{\pi'} = \square_{\pi \cup \pi'}$

(4) $\blacklozenge_\pi \blacklozenge_{\pi'} = \blacklozenge_{\pi \cup \pi'}$

(5) *If* $\pi \subseteq \pi'$, *then* $\square_{\pi'} \blacklozenge_\pi = \square_{\pi'}$.

(6) *If* $\pi \subseteq \pi'$, *then* $\blacklozenge_{\pi'} \square_\pi = \blacklozenge_{\pi'}$.

(7) *If* $\pi \cap \pi' = \emptyset$, *then* $\square_\pi \blacklozenge_{\pi'} = \blacklozenge_{\pi'} \square_\pi$.

(8) $\square_\pi \blacklozenge_{\pi'} = \blacklozenge_{\pi' - \pi} \square_\pi$.

(9) $\blacklozenge_\pi \square_{\pi'} = \square_{\pi' - \pi} \blacklozenge_\pi$.

# Conclusions

- One of the most abstract/philosophical parts of category theory, namely **axiomatic cohesion,** is a practical theory of information flow.
  - It can be used to prove properties of LBIFC…
  - … and, hopefully, it can inspire new languages for LBIFC. (notice there were no integral signs in the previous slide)
- Despite the looks of it, the use of **category theory** to reason about **programming languages** has not been exhausted—far from it.
- **Multi-modal type theories** have intuitive categorical semantics.