A Nominal Approach to Probabilistic Separation Logic

John Li
li.john@northeastern.edu

Jon Aytac
jmaytac@sandia.gov

Philip Johnson-Freyd
pajohn@sandia.gov

Amal Ahmed
amal@ccs.neu.edu

Steven Holtzen
s.holtzen@northeastern.edu

Northeastern University
Khoury College of Computer Sciences

Sandia National Laboratories

Lilac is a probabilistic separation logic

Lilac is a probabilistic separation logic

$$X \leftarrow \texttt{flip}\ 1/2;$$

$$Y \leftarrow \texttt{flip}\ 1/2;$$

$$X \sim \mathrm{Ber}(1/2) \quad * \quad Y \sim \mathrm{Ber}(1/2)$$

Lilac is a probabilistic separation logic

$X \leftarrow \texttt{flip}\ 1/2;$

$Y \leftarrow \texttt{flip}\ 1/2;$

$$X \sim \mathrm{Ber}(1/2) \quad * \quad Y \sim \mathrm{Ber}(1/2)$$

↑

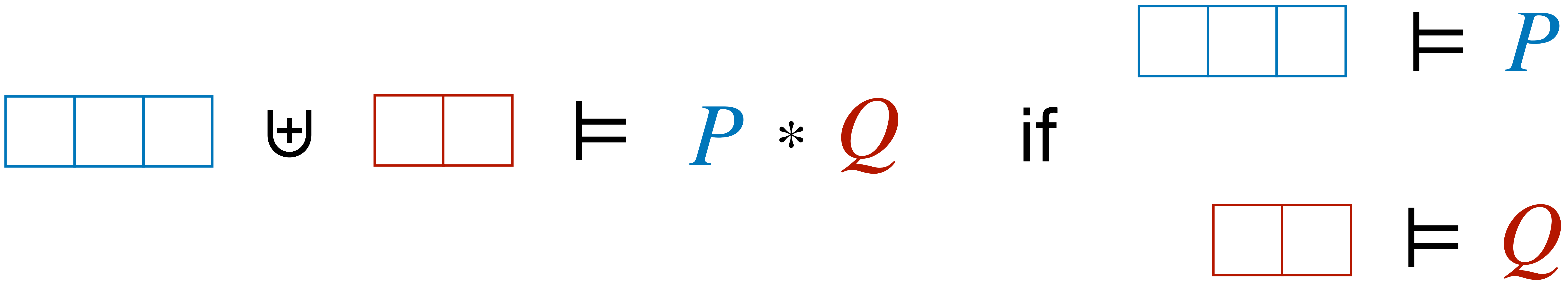
X and Y are independent random variables

The key idea

- Separate probability spaces into independent subspaces:

The key idea

- Separate probability spaces into independent subspaces:



The key idea

- Separate probability spaces into independent subspaces:

$$(\mathcal{F}, \mu) \bullet (\mathcal{G}, \nu) \vDash P * Q \quad \text{if} \quad \begin{matrix} (\mathcal{F}, \mu) \vDash P \\ (\mathcal{G}, \nu) \vDash Q \end{matrix}$$

The key idea

- Separate probability spaces into independent subspaces:

$$(\mathscr{F}, \mu) \bullet (\mathscr{G}, \nu) \models P * Q \quad \text{if} \quad \begin{array}{l} (\mathscr{F}, \mu) \models P \\ (\mathscr{G}, \nu) \models Q \end{array}$$

$\mathscr{F}, \mathscr{G}$ are σ-algebras,
μ, ν are probability measures

The key idea

- Separate probability spaces into independent subspaces:

$$(\mathscr{F}, \mu) \bullet (\mathscr{G}, \nu) \vDash P * Q \quad \text{if} \quad \begin{array}{c} (\mathscr{F}, \mu) \vDash P \\ (\mathscr{G}, \nu) \vDash Q \end{array}$$

independent combination
("disjoint union for spaces")

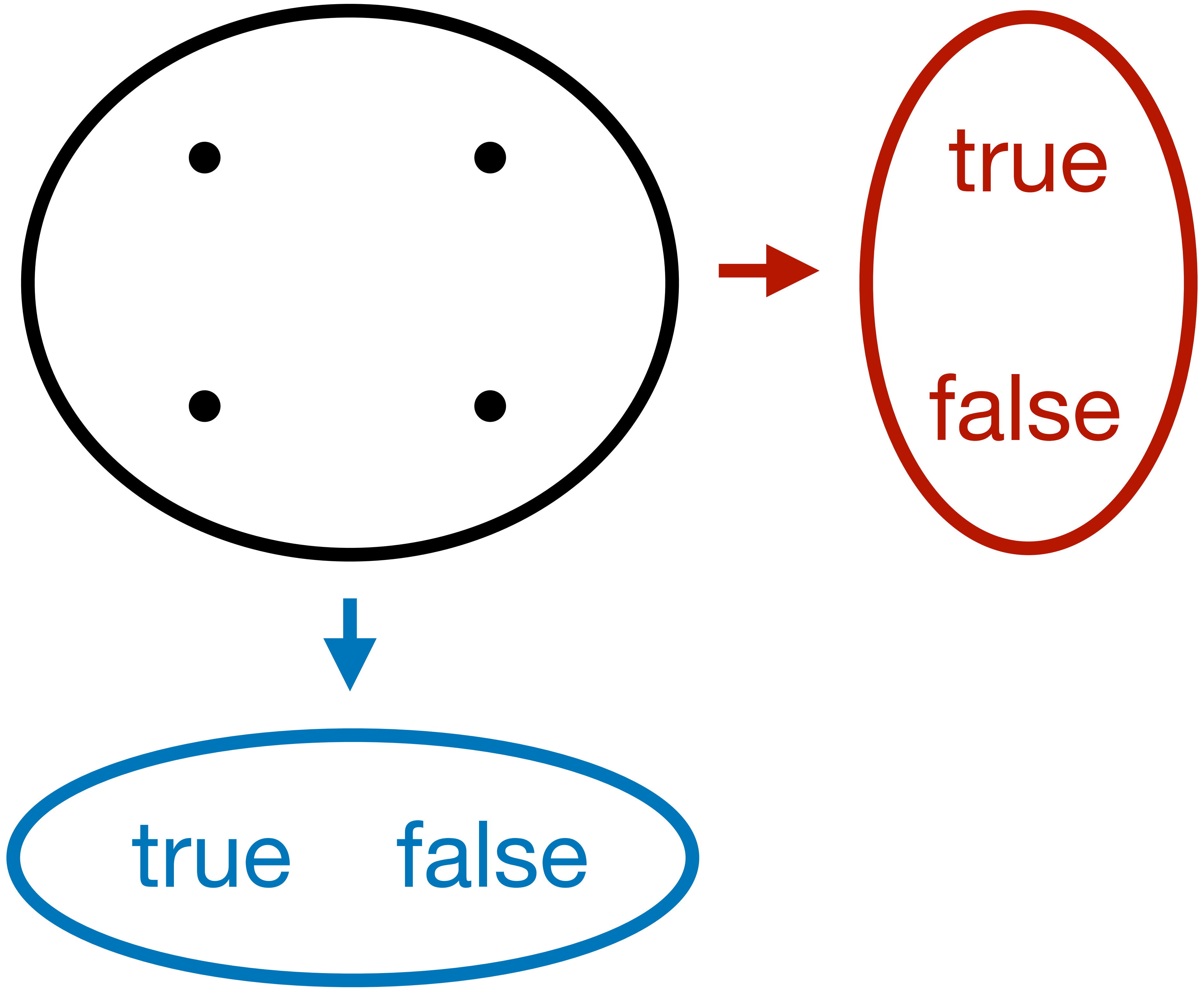
?!

?!

- Q: Why isn't separation just about product spaces?

?!

- Q: Why isn't separation just about product spaces?



This paper: a nominal answer

- Q: Why isn't separation just about product spaces?
- A: Actually, it is, up to a suitable equivalence of categories

This paper: a nominal answer

- Q: Why isn't separation just about product spaces?
- A: Actually, it is, up to a suitable equivalence of categories

EMS

"enhanced measurable sheaves"

This paper: a nominal answer

- Q: Why isn't separation just about product spaces?
- A: Actually, it is, up to a suitable equivalence of categories

$\mathbf{EMS}$

"enhanced measurable sheaves"

$\mathbf{Set}^{\ll}$

"absolutely continuous sets"

This paper: a nominal answer

- Q: Why isn't separation just about product spaces?
- A: Actually, it is, up to a suitable equivalence of categories

$\mathbf{EMS}$ $\quad\quad\quad$ $\mathrm{Set}^{\ll}$

independence via
product spaces

This paper: a nominal answer

- Q: Why isn't separation just about product spaces?
- A: Actually, it is, up to a suitable equivalence of categories

$\mathbf{EMS}$	$\mathbf{Set}^{\ll}$
independence via product spaces	Lilac's independent combination*

This paper: a nominal answer

- Q: Why isn't separation just about product spaces?
- A: Actually, it is, up to a suitable equivalence of categories

$$\mathbf{EMS} \simeq \mathbf{Set}^{\ll}$$

independence via product spaces		Lilac's independent combination*

This paper: a nominal answer

- Q: Why isn't separation just about product spaces?
- A: Actually, it is, up to a suitable equivalence of categories

$$\mathbf{EMS} \simeq \mathbf{Set}^{\ll}$$

independence via product spaces	$\sim$	Lilac's independent combination*

This paper: a nominal answer

- Q: Why isn't separation just about product spaces?
- A: Actually, it is, up to a suitable equivalence of categories
- We also work out this correspondence for discrete probability:

This paper: a nominal answer

- Q: Why isn't separation just about product spaces?
- A: Actually, it is, up to a suitable equivalence of categories
- We also work out this correspondence for discrete probability:

$\mathbf{EMS}_{\mathrm{d}}$

"discrete enhanced measurable sheaves"

This paper: a nominal answer

- Q: Why isn't separation just about product spaces?
- A: Actually, it is, up to a suitable equivalence of categories
- We also work out this correspondence for discrete probability:

$\mathbf{EMS}_{\mathrm{d}}$

"discrete enhanced measurable sheaves"

$\mathbf{Set}_{\mathrm{d}}^{\ll}$

"discrete absolutely continuous sets"

This paper: a nominal answer

- Q: Why isn't separation just about product spaces?
- A: Actually, it is, up to a suitable equivalence of categories
- We also work out this correspondence for discrete probability:

$$\mathbf{EMS}_{\mathrm{d}} \simeq \mathrm{Set}_{\mathrm{d}}^{\ll}$$

This paper: a nominal answer

- Q: Why isn't separation just about product spaces?
- A: Actually, it is, up to a suitable equivalence of categories
- We also work out this correspondence for discrete probability:

$$\mathbf{EMS}_{\mathrm{d}} \qquad \simeq \qquad \mathrm{Set}_{\mathrm{d}}^{\ll}$$

independence via product spaces	$\sim$	Lilac's independent combination, for discrete probability

The folklore

- Our results are probabilistic analogs of the following fact:

The folklore

- Our results are probabilistic analogs of the following fact:

$$\mathbf{Sch} = \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{Inj}^{\mathrm{op}}_{<\omega})$$

separation =
Day convolution wrt
coproduct

The folklore

- Our results are probabilistic analogs of the following fact:

$$\mathbf{Sch} = \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{Inj}^{\mathrm{op}}_{<\omega})$$

separation =
Day convolution wrt
coproduct

$$\mathbf{Nom} = \mathrm{Aut}_{<\omega}(\mathbb{N})\text{-sets}$$

separation = heaps
with disjoint domain

The folklore

- Our results are probabilistic analogs of the following fact:

$$\mathbf{Sch} = \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{Inj}^{\mathrm{op}}_{<\omega}) \quad \simeq \quad \mathbf{Nom} = \mathrm{Aut}_{<\omega}(\mathbb{N})\text{-sets}$$

separation =
Day convolution wrt
coproduct

separation = heaps
with disjoint domain

The folklore

- Our results are probabilistic analogs of the following fact:

$$\mathbf{Sch} = \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{Inj}_{<\omega}^{\mathrm{op}}) \quad \simeq \quad \mathbf{Nom} = \mathrm{Aut}_{<\omega}(\mathbb{N})\text{-sets}$$

separation = Day convolution wrt coproduct	$\sim$	separation = heaps with disjoint domain

A more abstract view: resources to atomic sheaves

A more abstract view: resources to atomic sheaves

$\mathbf{R}$

symmetric monoidal

"resources"

A more abstract view: resources to atomic sheaves

$\mathbf{R}$

$\mathbf{S}$

symmetric monoidal, atomic, ...

"resource shapes"

A more abstract view: resources to atomic sheaves

$$|\cdot| \quad : \quad \mathbf{R} \xrightarrow{\text{monoidal}} \mathbf{S}$$

"forget the contents of the resource"

A more abstract view: resources to atomic sheaves

$$|\cdot| \quad : \quad \mathbf{R} \xrightarrow{\text{monoidal}} \mathbf{S}$$

In $\mathrm{Sh}_{\mathrm{atomic}}(\mathbf{S})$,

$\mathrm{Res} = \varinjlim_{r:\mathrm{Core}(\mathbf{R})} \mathbf{S}(-, |r|)$ is a sheaf of resources

$\mathrm{Res} \otimes \mathrm{Res}$ is a sheaf of separated resources

A more abstract view: resources to atomic sheaves

$$|\cdot| \quad : \quad \mathbf{R} \xrightarrow{\text{monoidal}} \mathbf{S}$$

In $\mathrm{Sh}_{\mathrm{atomic}}(\mathbf{S})$,

$\mathrm{Res} = \varinjlim_{r:\mathrm{Core}(\mathbf{R})} \mathbf{S}(-, |r|)$ is a sheaf of resources

$\mathrm{Res} \otimes \mathrm{Res}$ is a sheaf of separated resources

Lemma C.23

A more abstract view: atomic sheaves to G-sets

- Under suitable conditions, one can find an object s_∞ that produces an equivalence $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{S}) \simeq \mathrm{Aut}(s_\infty)$-sets.

A more abstract view: atomic sheaves to G-sets

- Under suitable conditions, one can find an object s_∞ that produces an equivalence $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{S}) \simeq \mathrm{Aut}(s_\infty)$-sets.

- This equivalence gives a correspondence

$$\begin{array}{ccc} \mathrm{Res} \otimes \mathrm{Res} & & i(\mathrm{Res} \otimes \mathrm{Res}) \\ \text{in} & \sim & \text{in} \\ \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{S}) & & \mathrm{Aut}(s_\infty)\text{-sets.} \end{array}$$

Our probabilistic analog: the discrete case

Our probabilistic analog: the discrete case

- Resource = discrete probability space, shape = countable set

Our probabilistic analog: the discrete case

- Resource = discrete probability space, shape = countable set
- $|\cdot| =$ the functor $\mathbf{Prob}_{\leq\omega} \to \mathbf{Surj}_{\leq\omega}$ that forgets measures

Our probabilistic analog: the discrete case

- Resource = discrete probability space, shape = countable set
- $|\cdot| =$ the functor $\mathbf{Prob}_{\leq\omega} \to \mathbf{Surj}_{\leq\omega}$ that forgets measures
- $s_\infty = [0,1]$

Our probabilistic analog: the discrete case

- This yields $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{Surj}_{\leq\omega}) \simeq \mathrm{Aut}[0,1]$-sets

Our probabilistic analog: the discrete case

- This yields $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{Surj}_{\leq\omega}) \simeq \mathrm{Aut}[0,1]$-sets

$\mathbf{EMS}_{\mathrm{d}}$

Our probabilistic analog: the discrete case

- This yields $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{Surj}_{\leq\omega}) \simeq \mathrm{Aut}[0,1]$-sets

$\mathbf{EMS}_{\mathrm{d}}$ $\mathrm{Set}_{\mathrm{d}}^{\ll}$

Our probabilistic analog: the discrete case

- This yields $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{Surj}_{\leq\omega}) \simeq \mathrm{Aut}[0,1]$-sets

  $\mathbf{EMS}_{\mathrm{d}}$ $\mathrm{Set}_{\mathrm{d}}^{\ll}$

- Across this equivalence,

$$i(\mathrm{Res} \otimes \mathrm{Res}) = \left\{ \begin{array}{l} \text{independently combinable pairs of} \\ \text{discrete probability spaces on } [0,1] \end{array} \right\}$$

Our probabilistic analog: the discrete case

- This yields $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{Surj}_{\leq\omega}) \simeq \mathrm{Aut}[0,1]$-sets

  $\mathbf{EMS}_{\mathrm{d}}$ $\qquad\qquad$ $\mathrm{Set}_{\mathrm{d}}^{\ll}$

- Across this equivalence,

$$i(\mathrm{Res} \otimes \mathrm{Res}) = \left\{ \begin{array}{l} \text{independently combinable pairs of} \\ \text{discrete probability spaces on } [0,1] \end{array} \right\}$$

discrete independent combination comes from the monoidal structure on $\mathbf{Prob}_{\leq\omega}$

Our probabilistic analog: the discrete case

- This yields $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{Surj}_{\leq\omega}) \simeq \mathrm{Aut}[0,1]$-sets

- Across this equivalence,

$$i(\mathrm{Res} \otimes \mathrm{Res}) = \left\{ \begin{array}{l} \text{independently combinable pairs of} \\ \text{discrete probability spaces on } [0,1] \end{array} \right\}$$

Theorem 3.21

Our probabilistic analog: the continuous case

Our probabilistic analog: the continuous case

- Resource = standard probability space,
  Resource shape = enhanced measurable space

Our probabilistic analog: the continuous case

- Resource = standard probability space,
  Resource shape = enhanced measurable space
- $|\cdot| =$ the functor $\mathbf{Prob}_{\mathrm{std}} \to \mathbf{EMS}_{\mathrm{std}}$ that forgets measures

Our probabilistic analog: the continuous case

- Resource = standard probability space,
  Resource shape = enhanced measurable space
- $|\cdot| =$ the functor $\mathbf{Prob}_{\mathrm{std}} \to \mathbf{EMS}_{\mathrm{std}}$ that forgets measures
- $s_\infty = [0,1]^\omega$

Our probabilistic analog: the continuous case

- This yields $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{EMS}_{\mathrm{std}}) \simeq \mathrm{Aut}[0,1]^{\omega}$-sets

Our probabilistic analog: the continuous case

- This yields $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{EMS}_{\mathrm{std}}) \simeq \mathrm{Aut}[0,1]^{\omega}$-sets

$\mathbf{EMS}$

Our probabilistic analog: the continuous case

- This yields $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{EMS}_{\mathrm{std}}) \simeq \mathrm{Aut}[0,1]^{\omega}$-sets

$\mathbf{EMS}$ $\mathrm{Set}^{\ll}$

Our probabilistic analog: the continuous case

- This yields $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{EMS}_{\mathrm{std}}) \simeq \mathrm{Aut}[0,1]^{\omega}$-sets

$\mathbf{EMS}$ $\mathrm{Set}^{\ll}$

- Across this equivalence,

$$i(\mathrm{Res} \otimes \mathrm{Res}) = \left\{ \begin{array}{l} \text{independently combinable pairs of} \\ \text{finite-width probability spaces on } [0,1]^{\omega} \end{array} \right\}$$

Our probabilistic analog: the continuous case

- This yields $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{EMS}_{\mathrm{std}}) \simeq \mathrm{Aut}[0,1]^{\omega}$-sets

$\mathbf{EMS}$ $\mathbf{Set}^{\ll}$

- Across this equivalence,

$$i(\mathrm{Res} \otimes \mathrm{Res}) = \left\{ \begin{array}{l} \text{independently combinable pairs of} \\ \text{finite-width probability spaces on } [0,1]^{\omega} \end{array} \right\}$$

Lilac's independent combination comes from the monoidal structure on $\mathbf{Prob}_{\mathrm{std}}$

Our probabilistic analog: the continuous case

- This yields $i : \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{EMS}_{\mathrm{std}}) \simeq \mathrm{Aut}[0,1]^{\omega}$-sets

- Across this equivalence,

$$i(\mathrm{Res} \otimes \mathrm{Res}) = \left\{ \begin{array}{l} \text{independently combinable pairs of} \\ \text{finite-width probability spaces on } [0,1]^{\omega} \end{array} \right\}$$

Theorem 4.24

See the paper for...

- Precise definitions
- Separation logic details
- Constructing suitable s_∞s
- Properties of $\mathbf{EMS}_{\mathrm{std}}$ (monoidal, atomic, subcanonical)

Summary

Summary

- Lilac's independent combination can be explained in terms of the familiar product of probability spaces

Summary

- Lilac's independent combination can be explained in terms of the familiar product of probability spaces
- Our nominal-flavored equivalences corroborate recent work relating probability to names

Summary

- Lilac's independent combination can be explained in terms of the familiar product of probability spaces
- Our nominal-flavored equivalences corroborate recent work relating probability to names

Probabilistic Programming Semantics for Name Generation

MARCIN SABOK, McGill University, Canada
SAM STATON, University of Oxford, United Kingdom
DARIO STEIN, University of Oxford, United Kingdom
MICHAEL WOLMAN, McGill University, Canada

Equivalence and Conditional Independence in Atomic Sheaf Logic

Alex Simpson*

Probability Sheaves and the Giry Monad*

Alex Simpson

li.john@northeastern.edu

Thanks!

$\mathbf{EMS}$	$\simeq$	$\mathrm{Set}^{\ll}$
independence via product spaces	$\sim$	Lilac's independent combination*

The folklore

- Our results are probabilistic analogs of the following fact:

The folklore

- Our results are probabilistic analogs of the following fact:

$$\text{separation logic in } \mathbf{Sch} \qquad \simeq \qquad \text{separation logic in } \mathbf{Nom}$$

The folklore

- Our results are probabilistic analogs of the following fact:

separation logic in **Sch** $\simeq$ separation logic in **Nom**

The folklore: separation logic in **Sch**

- $\mathbf{Sch} = \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{FinInj}^{\mathrm{op}})$

The folklore: separation logic in **Sch**

- $\mathbf{Sch} = \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{FinInj}^{\mathrm{op}})$

"heap shapes"

The folklore: separation logic in **Sch**

- $\mathbf{Sch} = \mathrm{Sh}_{\mathrm{atomic}}(\mathbf{FinInj}^{\mathrm{op}})$
- $(\mathbf{FinInj}^{\mathrm{op}}, +, \varnothing)$ is a monoidal category.
- Yields a monoidal structure $(\otimes, \mathrm{I})$ on $\mathbf{Sch}$, by Day convolution.

The folklore: separation logic in **Sch**

- There is a sheaf of heaps $\mathbb{H}(L) = L \rightharpoonup_{\mathrm{fin}} \mathbb{Z}$.
- The convolution $\mathbb{H} \otimes \mathbb{H}$ is a sheaf of separated heaps:

$$(\mathbb{H} \otimes \mathbb{H})(L) = \{(h, h') \mid \mathrm{dom}(h) \cap \mathrm{dom}(h') = \varnothing\}$$

- These form the basic ingredients of separation logic.

The folklore: separation logic in **Sch**

- Our results are probabilistic analogs of the following fact:

separation logic in **Sch** $\simeq$ separation logic in **Nom**

The folklore: separation logic in **Nom**

- Our results are probabilistic analogs of the following fact:

separation logic in **Sch** $\simeq$ separation logic in **Nom**

The folklore: separation logic in **Nom**

- $\mathbf{Nom} = \mathbf{G}\ \mathrm{Set}$, where $\mathbf{G} = \mathrm{Aut}_{\mathrm{fin}}(\mathbb{N})$ + a particular topology.

The folklore: separation logic in **Nom**

- $\mathbf{Nom} = \mathbf{G}\ \mathcal{S}\mathrm{et}$, where $\mathbf{G} = \mathrm{Aut}_{\mathrm{fin}}(\mathbb{N})$ + a particular topology.
- Heaps: $\overline{\mathbb{H}} = \mathbb{N} \rightharpoonup_{\mathrm{fin}} \mathbb{Z}$
- Separated heaps:

$$\overline{\mathbb{H}}_{\mathrm{sep}} = \{(h, h') \in \overline{\mathbb{H}} \times \overline{\mathbb{H}} \mid \mathrm{dom}(h) \cap \mathrm{dom}(h') = \varnothing\}$$

- These again form the basic ingredients of separation logic.

The folklore: separation logic in **Nom**

- Our results are probabilistic analogs of the following fact:

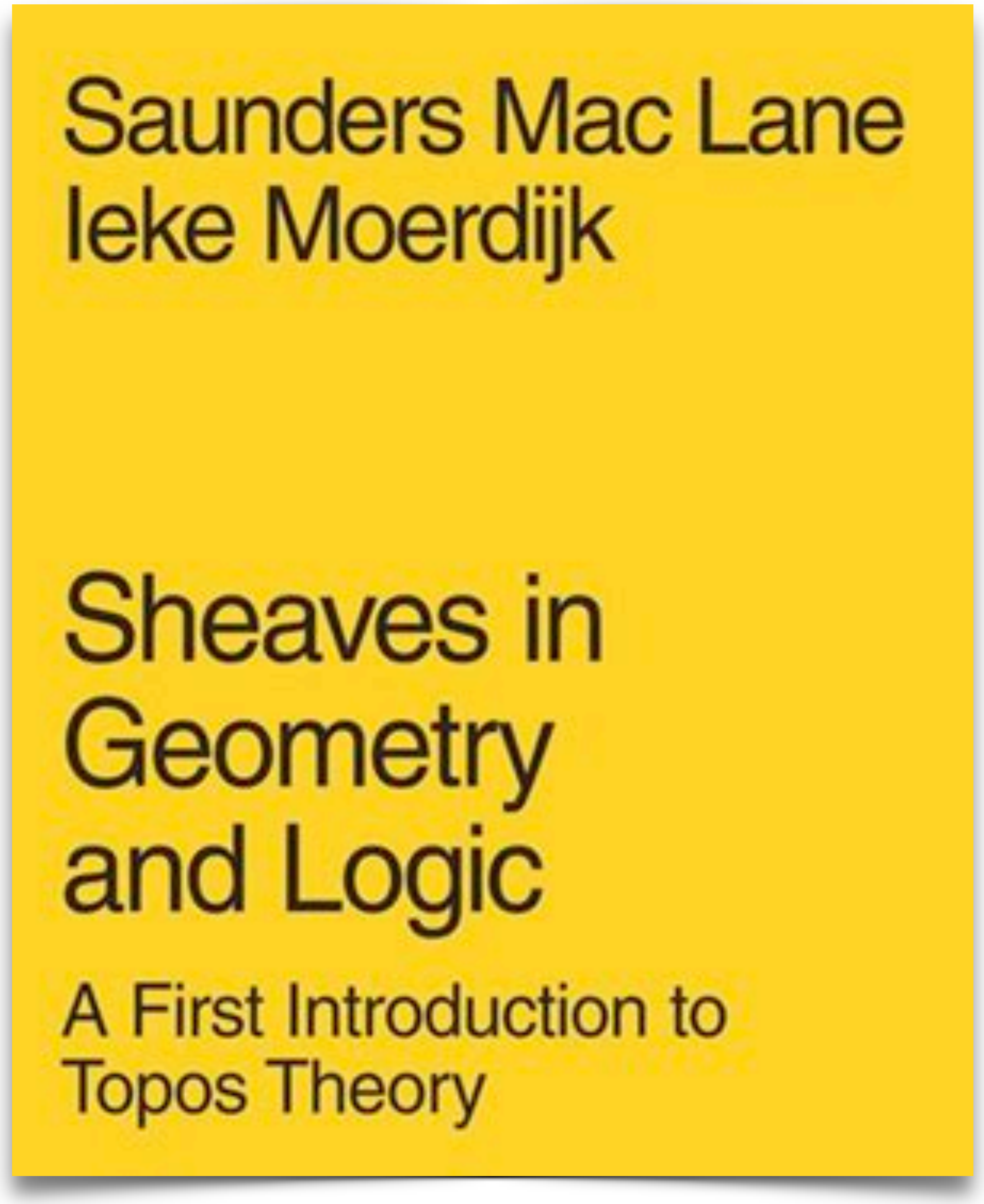
separation logic in **Sch** $\simeq$ separation logic in **Nom**

The folklore: the equivalence

- Our results are probabilistic analogs of the following fact:

separation logic in **Sch** $\simeq$ separation logic in **Nom**

The folklore: the equivalence



, Theorem III.9.2: $\mathbf{Sch} \simeq \mathbf{Nom}$.

The folklore: the equivalence

- Across this equivalence,

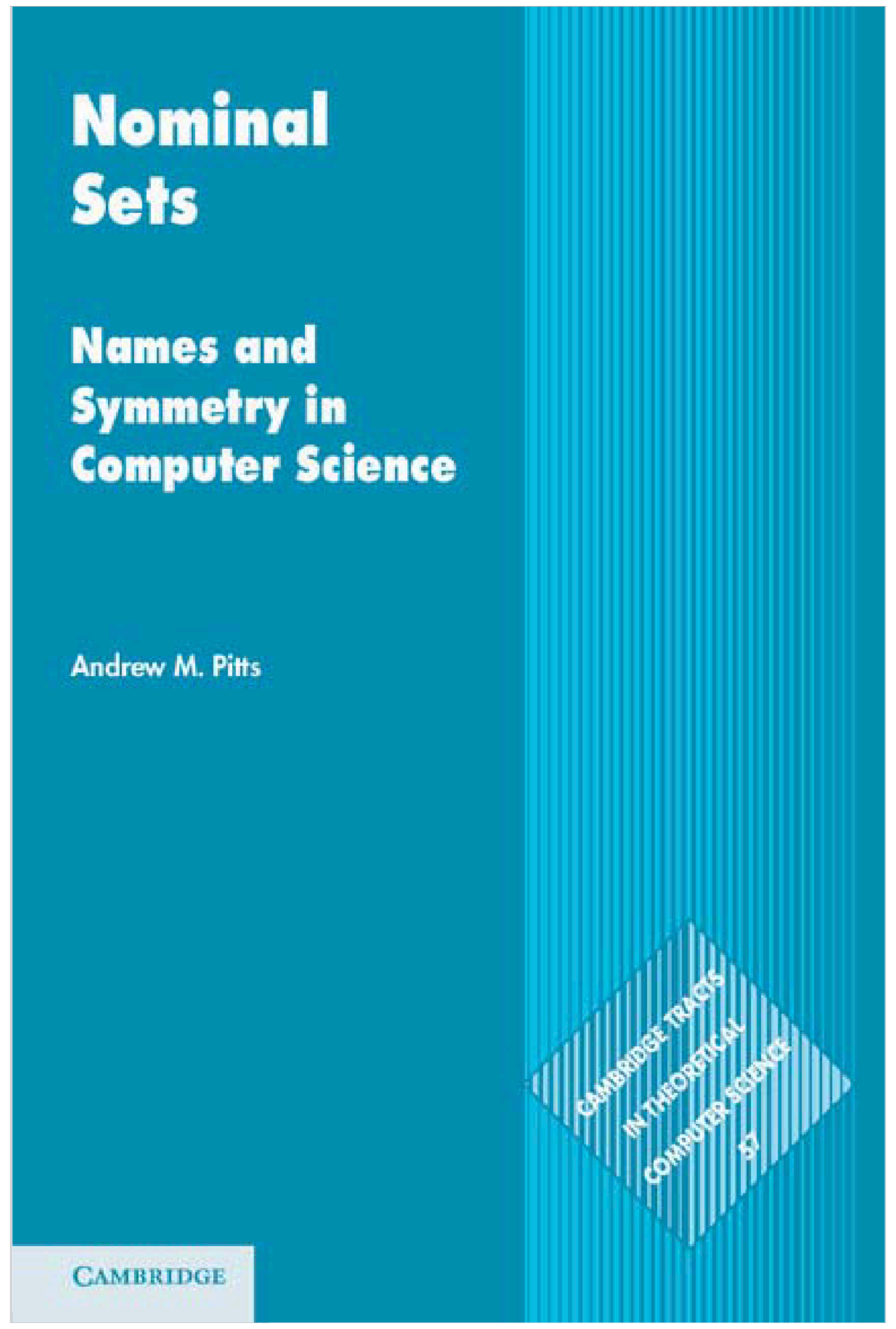
$\mathbf{Sch}$		$\mathbf{Nom}$
$\mathbb{H}$	corresponds to	$\overline{\mathbb{H}}$
$\mathbb{H} \otimes \mathbb{H}$	corresponds to	$\overline{\mathbb{H}}_{\mathrm{sep}}$

The folklore: the equivalence

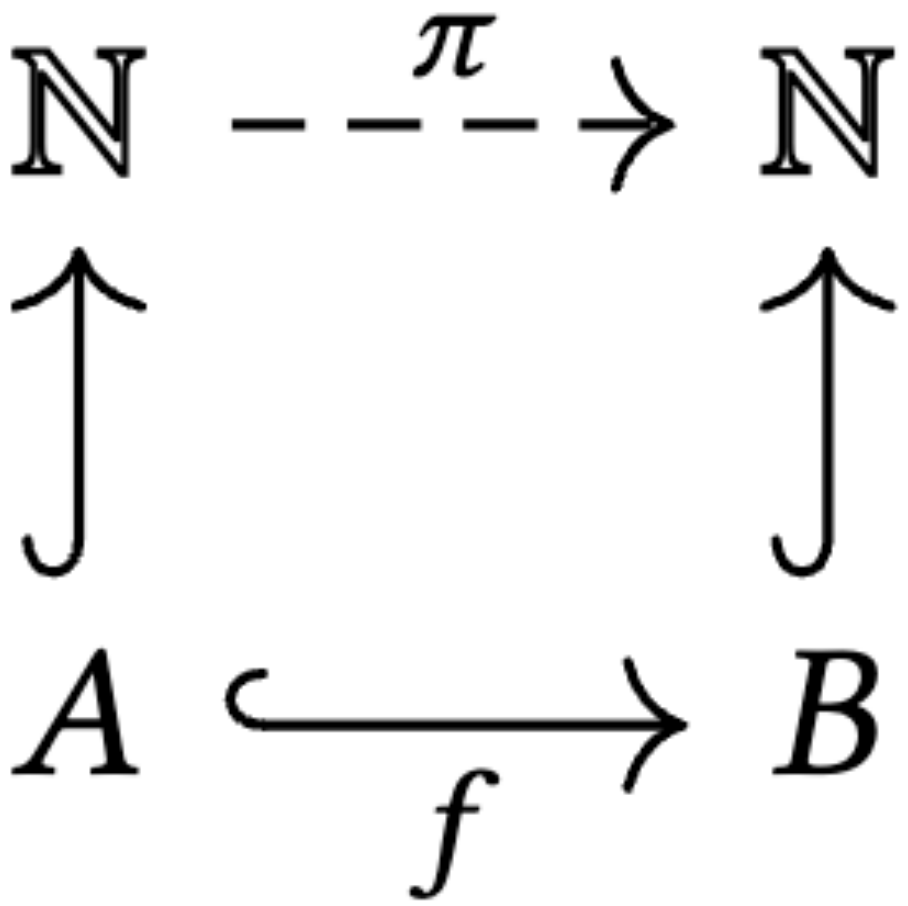
- Key idea: every renaming can be implemented by a permutation

The folklore: the equivalence

- Key idea: every renaming can be implemented by a permutation



, Lemma 1.14 (Homogeneity):



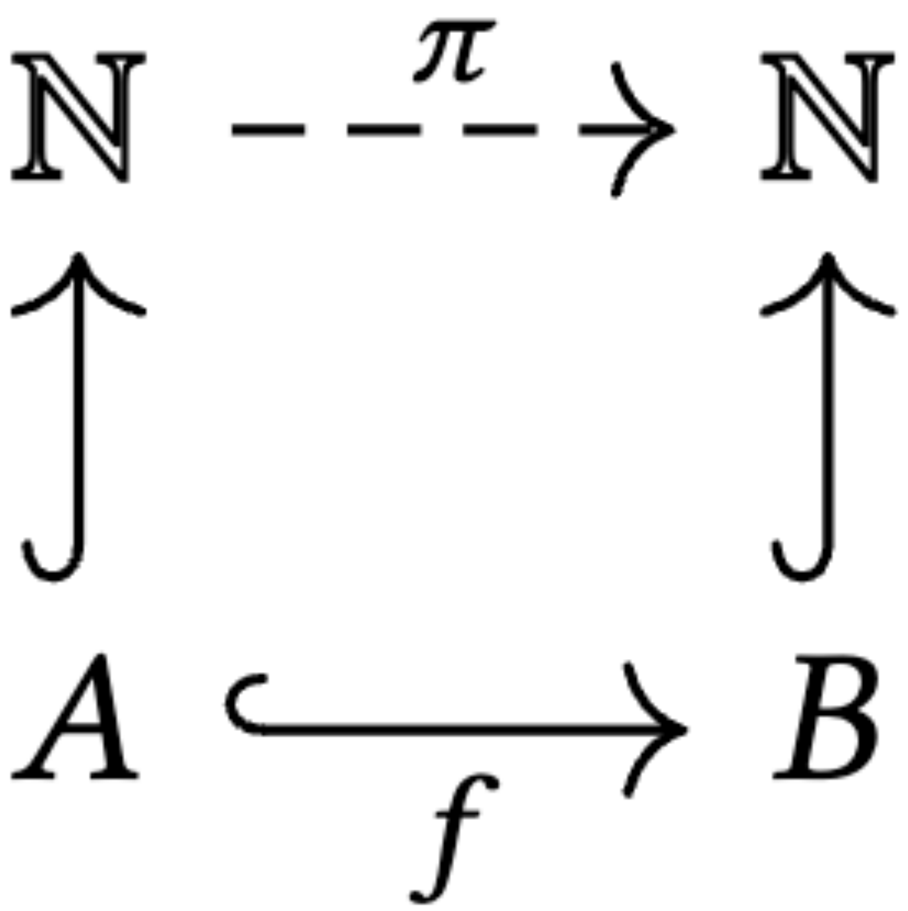
Our probabilistic analog: the discrete case

- Key lemma:

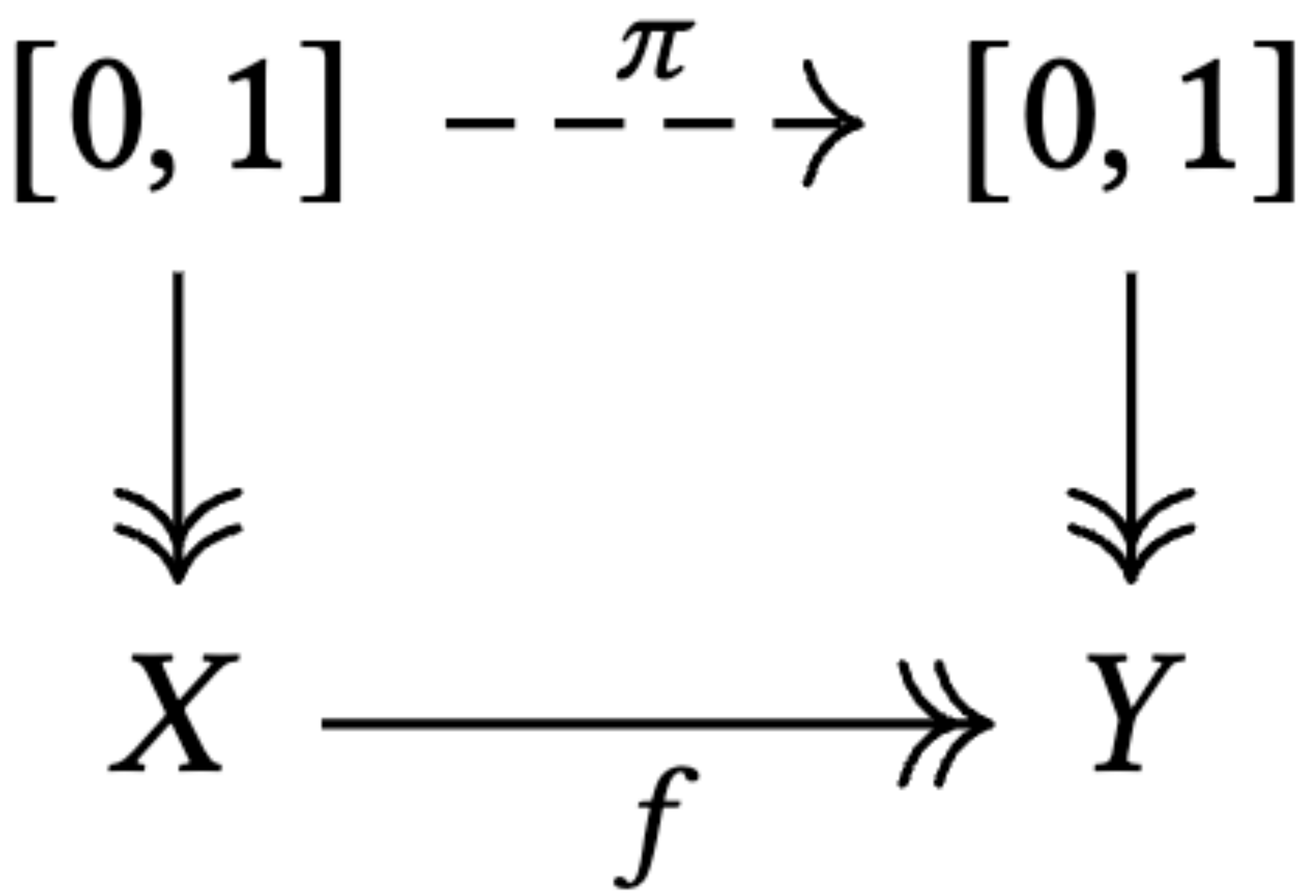
$$
\begin{array}{ccc}
\mathbb{N} & \overset{\pi}{\dashrightarrow} & \mathbb{N} \\
\uparrow & & \uparrow \\
A & \underset{f}{\hookrightarrow} & B
\end{array}
\quad \text{becomes} \quad
\begin{array}{ccc}
[0,1] & \overset{\pi}{\dashrightarrow} & [0,1] \\
\downarrow & & \downarrow \\
X & \underset{f}{\twoheadrightarrow} & Y
\end{array}
$$

Our probabilistic analog: the discrete case

- Key lemma:



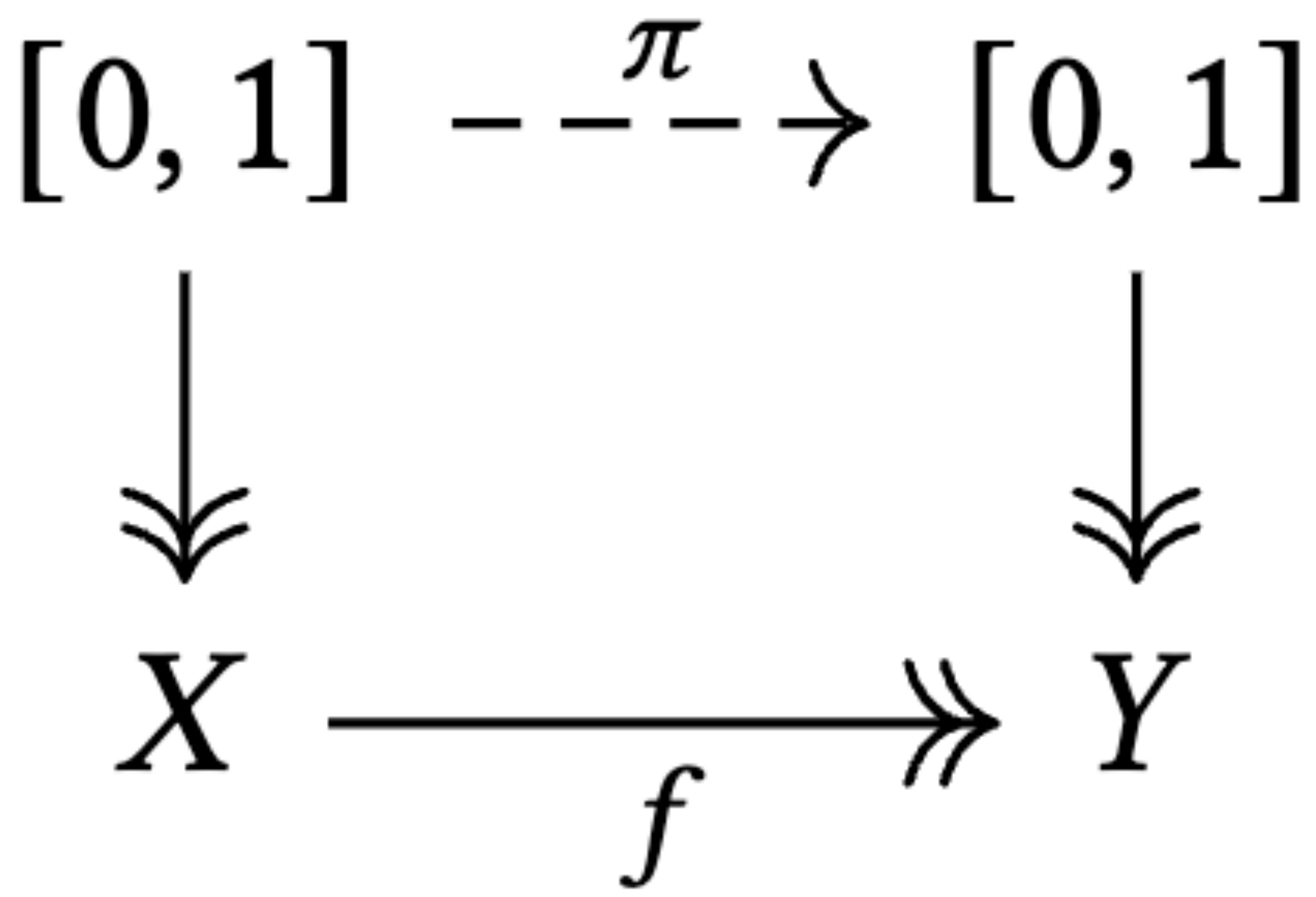
becomes



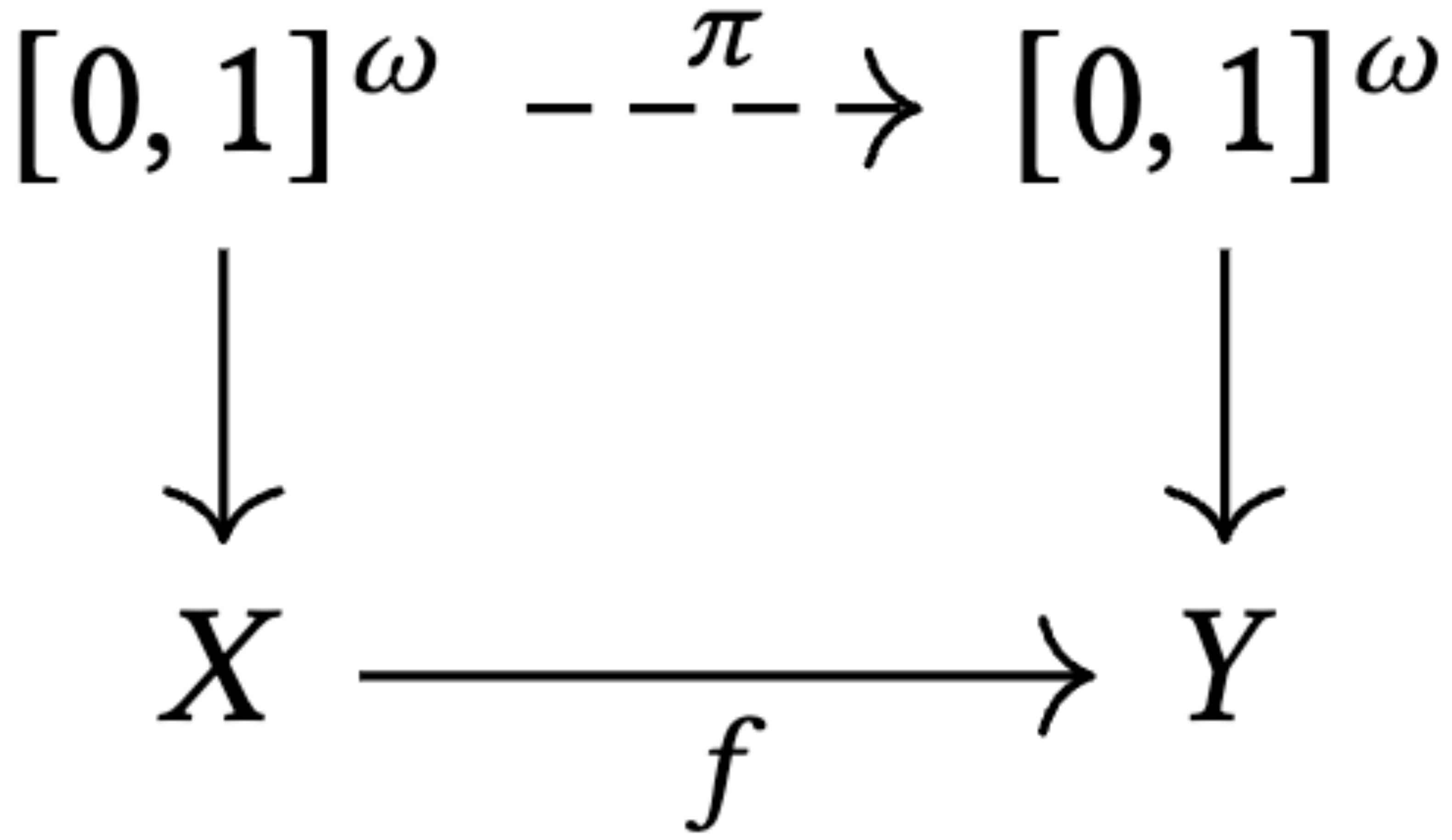
- Proof roughly boils down to: any two nonnegligible measurable subsets of $[0,1]$ are measurably isomorphic.

Our probabilistic analog: the continuous case

- Key lemma:



becomes



Our probabilistic analog: the continuous case

- Key lemma:

$$\begin{array}{ccc} [0,1] & \overset{\pi}{\dashrightarrow} & [0,1] \\ \big\downarrow & & \big\downarrow \\ X & \underset{f}{\twoheadrightarrow} & Y \end{array} \qquad \text{becomes} \qquad \begin{array}{ccc} [0,1]^{\omega} & \overset{\pi}{\dashrightarrow} & [0,1]^{\omega} \\ \big\downarrow & & \big\downarrow \\ X & \underset{f}{\longrightarrow} & Y \end{array}$$

- Proof requires some heavy-duty measure theory.