Towards a Categorical Model of the Lilac 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

- In ordinary separation logic,

$$x = \mathsf{new}\ 0;$$

$$y = \mathsf{new}\ 1;$$

$$(x \mapsto 0) \ * \ (y \mapsto 1)$$

Lilac is a probabilistic separation logic

- In ordinary separation logic,

$$x = \mathsf{new}\ 0;$$

$$y = \mathsf{new}\ 1;$$

$$(x \mapsto 0) \quad * \quad (y \mapsto 1)$$

x and y point to disjoint heap locations

Lilac is a probabilistic separation logic

- In 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

- In 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

Lilac is a probabilistic separation logic

- Lilac's separation is complete for independence

Lilac is a probabilistic separation logic

- Lilac's separation is complete for independence
- We used Lilac to verify a weighted sampling algorithm

Lilac is a probabilistic separation logic

- Lilac's separation is complete for independence
- We used Lilac to verify a weighted sampling algorithm
- For more, see:

Lilac: A Modal Separation Logic for Conditional Probability

JOHN M. LI, Northeastern University, USA
AMAL AHMED, Northeastern University, USA
STEVEN HOLTZEN, Northeastern University, USA

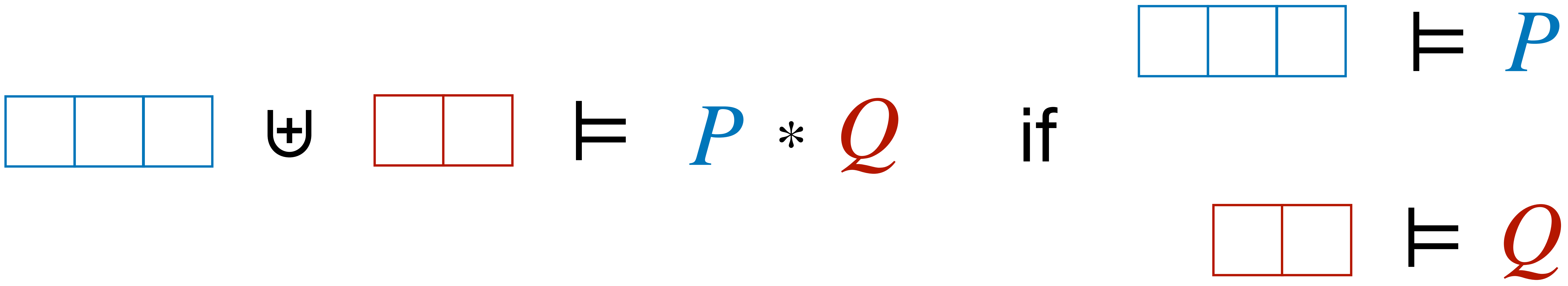
PLDI'23

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:

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

The key idea

- Separate probability spaces into independent subspaces:

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

independent combination
("disjoint union for spaces")

The fine print

Proof. $\mathbf{1}$ is indeed a unit: if $(\mathcal{F}, \mu)$ is some other probability space on Ω then $\langle \mathcal{F}, \mathcal{F}_{\mathbf{1}} \rangle = \mathcal{F}$ and μ witnesses the independent combination of itself with $\mu_{\mathbf{1}}$. And the relation "$\mathcal{P}$ is an independent combination of Q and $\mathcal{R}$" is clearly symmetric in Q and $\mathcal{R}$, so $(\bullet)$ is commutative. We just need to show $(\bullet)$ is associative and respects $(\sqsubseteq)$.

For associativity, suppose $(\mathcal{F}_1, \mu_1) \bullet (\mathcal{F}_2, \mu_2) = (\mathcal{F}_{12}, \mu_{12})$ and $(\mathcal{F}_{12}, \mu_{12}) \bullet (\mathcal{F}_3, \mu_3) = (\mathcal{F}_{(12)3}, \mu_{(12)3})$. There are three things to check:

- Some μ_{23} witnesses the combination of $(\mathcal{F}_2, \mu_2)$ and $(\mathcal{F}_3, \mu_3)$.
- Some $\mu_{1(23)}$ witnesses the combination of $(\mathcal{F}_1, \mu_1)$ and $(\mathcal{F}_{23}, \mu_{23})$.
- $(\langle \mathcal{F}_1, \langle \mathcal{F}_2, \mathcal{F}_3 \rangle \rangle, \mu_{1(23)}) = (\langle \langle \mathcal{F}_1, \mathcal{F}_2 \rangle, \mathcal{F}_3 \rangle, \mu_{(12)3})$.

We'll show this as follows:

(1) $\langle \mathcal{F}_1, \langle \mathcal{F}_2, \mathcal{F}_3 \rangle \rangle = \langle \langle \mathcal{F}_1, \mathcal{F}_2 \rangle, \mathcal{F}_3 \rangle$.
(2) Define $\mu_{23} := \mu_{(12)3}|_{\mathcal{F}_{23}}$. This is a witness for $(\mathcal{F}_2, \mu_2)$ and $(\mathcal{F}_3, \mu_3)$.
(3) Define $\mu_{1(23)} := \mu_{(12)3}$. This is a witness for $(\mathcal{F}_1, \mu_1)$ and $(\mathcal{F}_{23}, \mu_{23})$.

To show the left-to-right inclusion for (1): by the universal property of freely-generated σ-algebras, we just need to show $\langle \langle \mathcal{F}_1, \mathcal{F}_2 \rangle, \mathcal{F}_3 \rangle$ is a σ-algebra containing $\mathcal{F}_1$ and $\langle \mathcal{F}_2, \mathcal{F}_3 \rangle$. It clearly contains $\mathcal{F}_1$. To show it contains $\langle \mathcal{F}_2, \mathcal{F}_3 \rangle$, we just need to show it contains $\mathcal{F}_2$ and $\mathcal{F}_3$ (by the universal property again), which it clearly does. The right-to-left inclusion is similar.

For (2), if $E_2 \in \mathcal{F}_2$ and $E_3 \in \mathcal{F}_3$ then $\mu_{23}(E_2 \cap E_3) = \mu_{(12)3}(E_2 \cap E_3) = \mu_{(12)3}((\Omega \cap E_2) \cap E_3) = \mu_{12}(\Omega \cap E_2)\mu_3(E_3) = \mu_1(\Omega)\mu_2(E_2)\mu_3(E_3) = \mu_2(E_2)\mu_3(E_3)$ as desired.

For (3), we need $\mu_{(12)3}(E_1 \cap E_{23}) = \mu_1(E_1)\mu_{23}(E_{23})$ for all $E_1 \in \mathcal{F}_1$ and $E_{23} \in \langle \mathcal{F}_2, \mathcal{F}_3 \rangle$. For this we use the π-λ theorem. Let $\mathcal{E}$ be the set $\{E_2 \cap E_3 \mid E_2 \in \mathcal{F}_2, E_3 \in \mathcal{F}_3\}$ of intersections of events in $\mathcal{F}_2$ and $\mathcal{F}_3$. $\mathcal{E}$ is a π-system that generates $\langle \mathcal{F}_2, \mathcal{F}_3 \rangle$ (lemma B.2). Let $\mathcal{G}$ be the set of events E_{23} such that $\mu_{(12)3}(E_1 \cap E_{23}) = \mu_1(E_1)\mu_{23}(E_{23})$ for all $E_1 \in \mathcal{F}_1$. We are done if $\langle \mathcal{E} \rangle \subseteq \mathcal{G}$. By the π-λ theorem, we just need to check that $\mathcal{E} \subseteq \mathcal{G}$ and that $\mathcal{G}$ is a λ-system. We have $\mathcal{E} \subseteq \mathcal{G}$ because if $E_2 \in \mathcal{F}_2$ and $E_3 \in \mathcal{F}_3$ then $\mu_{(12)3}(E_1 \cap (E_2 \cap E_3)) = \mu_1(E_1)\mu_2(E_2)\mu_3(E_3) = \mu_1(E_1)\mu_{23}(E_2 \cap E_3)$. To see that $\mathcal{G}$ is a λ-system, note that $\mu_1(E_1)\mu_{23}(E_{23}) = \mu_{(12)3}(E_1)\mu_{(12)3}(E_{23})$ and so $\mathcal{G}$ is actually equal to $\mathcal{F}_1^{\perp}$ (the set of events independent of $\mathcal{F}_1$), a λ-system by Lemma B.3.

To show $(\bullet)$ respects $(\sqsubseteq)$, suppose $(\mathcal{F}, \mu) \sqsubseteq (\mathcal{F}', \mu')$ and $(\mathcal{G}, \nu) \sqsubseteq (\mathcal{G}', \nu')$ and $(\mathcal{F}', \mu') \bullet (\mathcal{G}', \nu') = (\langle \mathcal{F}', \mathcal{G}' \rangle, \rho')$. We need to show (1) $(\mathcal{F}, \mu) \bullet (\mathcal{G}, \nu) = (\langle \mathcal{F}, \mathcal{G} \rangle, \rho)$ and (2) $(\langle \mathcal{F}, \mathcal{G} \rangle, \rho) \sqsubseteq (\langle \mathcal{F}', \mathcal{G}' \rangle, \rho')$ for some ρ. Define ρ to be the restriction of ρ' to $\langle \mathcal{F}, \mathcal{G} \rangle$. Now (1) holds because $\rho(F \cap G) = \rho'(F \cap G) = \rho'(F)\rho'(G) = \rho(F)\rho(G)$ for all $F \in \mathcal{F}$ and $G \in \mathcal{G}$ (the second step follows from $\mathcal{F} \subseteq \mathcal{F}'$ and $\mathcal{G} \subseteq \mathcal{G}'$). For (2), $\langle \mathcal{F}, \mathcal{G} \rangle \subseteq \langle \mathcal{F}', \mathcal{G}' \rangle$ because $\mathcal{F} \subseteq \mathcal{F}'$ and $\mathcal{G} \subseteq \mathcal{G}'$, and $\rho = \rho'|_{\langle \mathcal{F}, \mathcal{G} \rangle}$ by construction. □

The fine print

THEOREM B.25. *Let $\mathcal{M}_{\text{disintegrable}}$ be the set of countably-generated probability spaces $\mathcal{P}$ that have finite footprint and can be extended to a Borel measure on the entire Hilbert cube. The restriction of the KRM given by Theorem 2.4 to $\mathcal{M}_{\text{disintegrable}}$ is still a KRM.*

The fine print

THEOREM B.25. *Let $\mathcal{M}_{\text{disintegrable}}$ be the set of countably-generated probability spaces $\mathcal{P}$ that have finite footprint and can be extended to a Borel measure on the entire Hilbert cube. The restriction of the KRM given by Theorem 2.4 to $\mathcal{M}_{\text{disintegrable}}$ is still a KRM.*

The fine print

THEOREM B.25. *Let $\mathcal{M}_{\text{disintegrable}}$ be the set of countably-generated probability spaces $\mathcal{P}$ that have finite footprint and can be extended to a Borel measure on the entire Hilbert cube. The restriction of the KRM given by Theorem 2.4 to $\mathcal{M}_{\text{disintegrable}}$ is still a KRM.*

The fine print

THEOREM B.25. *Let* $\mathcal{M}_{\text{disintegrable}}$ *be the set of countably-generated probability spaces* $\mathcal{P}$ *that have finite footprint and can be extended to a Borel measure on the entire Hilbert cube. The restriction of the KRM given by Theorem 2.4 to* $\mathcal{M}_{\text{disintegrable}}$ *is still a KRM.*

The fine print

THEOREM B.25. *Let $\mathcal{M}_{\text{disintegrable}}$ be the set of countably-generated probability spaces $\mathcal{P}$ that have finite footprint and can be extended to a Borel measure on the entire Hilbert cube. The restriction of the KRM given by Theorem 2.4 to $\mathcal{M}_{\text{disintegrable}}$ is still a KRM.*

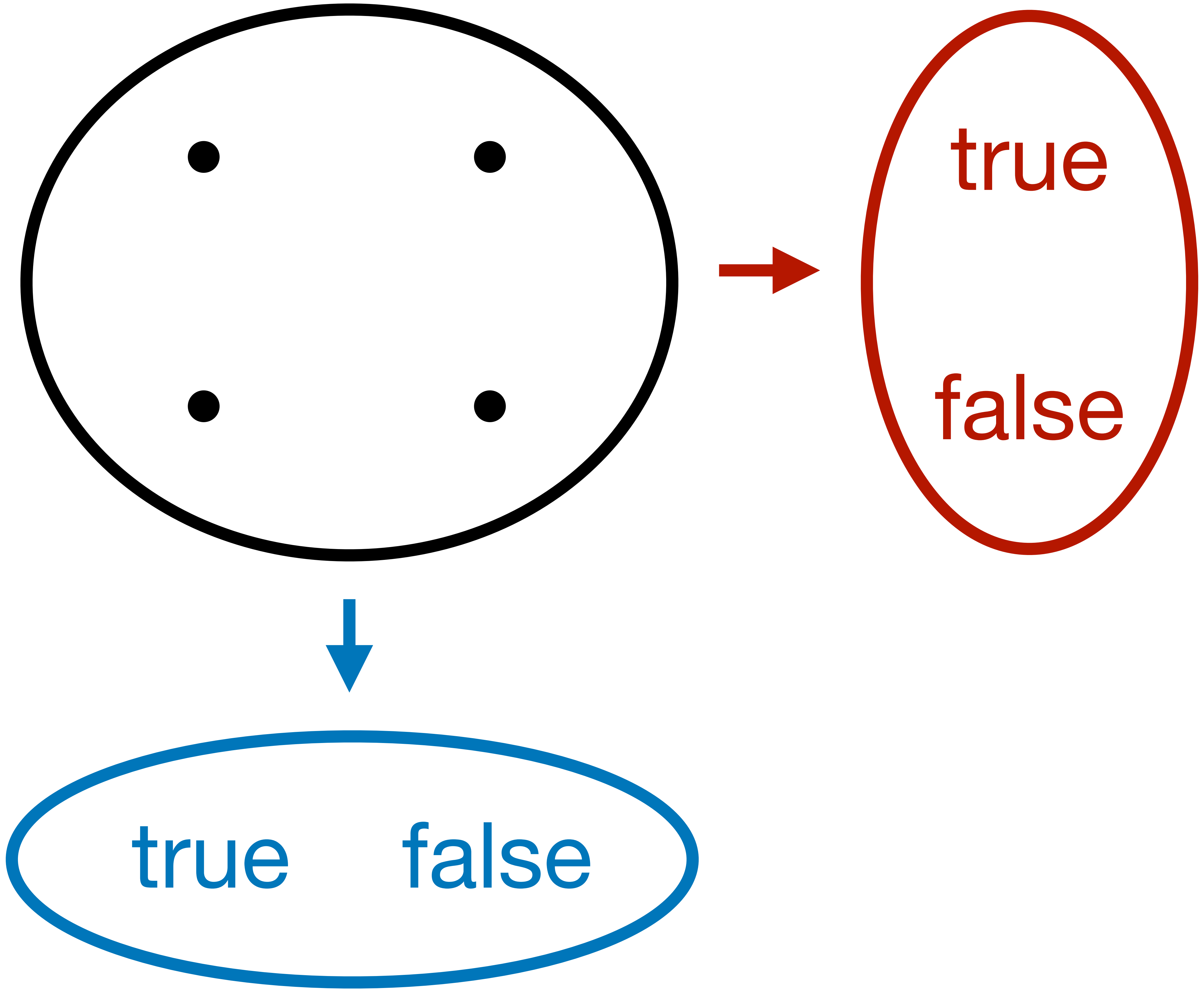
?!

?!

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

?!

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



?!

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

Towards a categorical answer

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

Towards a categorical answer

- Q: Why isn't separation just about product spaces?
- A: It **is** just about product spaces... up to a suitable equivalence of categories

First, some history...

First, some history...

- Today, the standard model of separation is heap-disjoint-union.

First, some history...

- Today, the standard model of separation is heap-disjoint-union.
- But it didn't always used to be this way:

First, some history...

- Today, the standard model of separation is heap-disjoint-union.
- But it didn't always used to be this way:

A Model for Syntactic Control of Interference

P. W. O'Hearn
School of Computer and Information Science
Syracuse University, Syracuse, NY, USA 13224-4100

MSCS'93

First, some history...

- Today, the standard model of separation is heap-disjoint-union.
- But it didn't always used to be this way:

6.1. The Tensor Product

The bifunctor $\otimes$ on $\mathbf{K}$ is a subfunctor of the categorical product $\times$, restricted so that different components are independent of one another.

If A, B are $\mathbf{K}$-objects then

$$
\begin{aligned}
(A \otimes B)X &= \{(a, b) \in A(X) \times B(X) \mid a \triangle b\}, \text{ ordered componentwise} \\
(A \otimes B)\, f\, (a, b) &= (A(f)\, a, B(f)\, b)
\end{aligned}
$$

First, some history...

- Today, the standard model of separation is heap-disjoint-union.
- But it didn't always used to be this way:

6.1. The Tensor Product

The bifunctor $\otimes$ on $\mathbf{K}$ is a subfunctor of the categorical product $\times$, restricted so that different components are independent of one another.

Day convolution w.r.t. coproduct of heap shapes

First, some history...

- Today, the standard model of separation is heap-disjoint-union.
- But it didn't always used to be this way:

the Schanuel topos* **Sch**

6.1. The Tensor Product

The bifunctor $\otimes$ on $\mathbf{K}$ is a subfunctor of the categorical product $\times$, restricted so that different components are independent of one another.

Day convolution w.r.t. coproduct of heap shapes

First, some history...

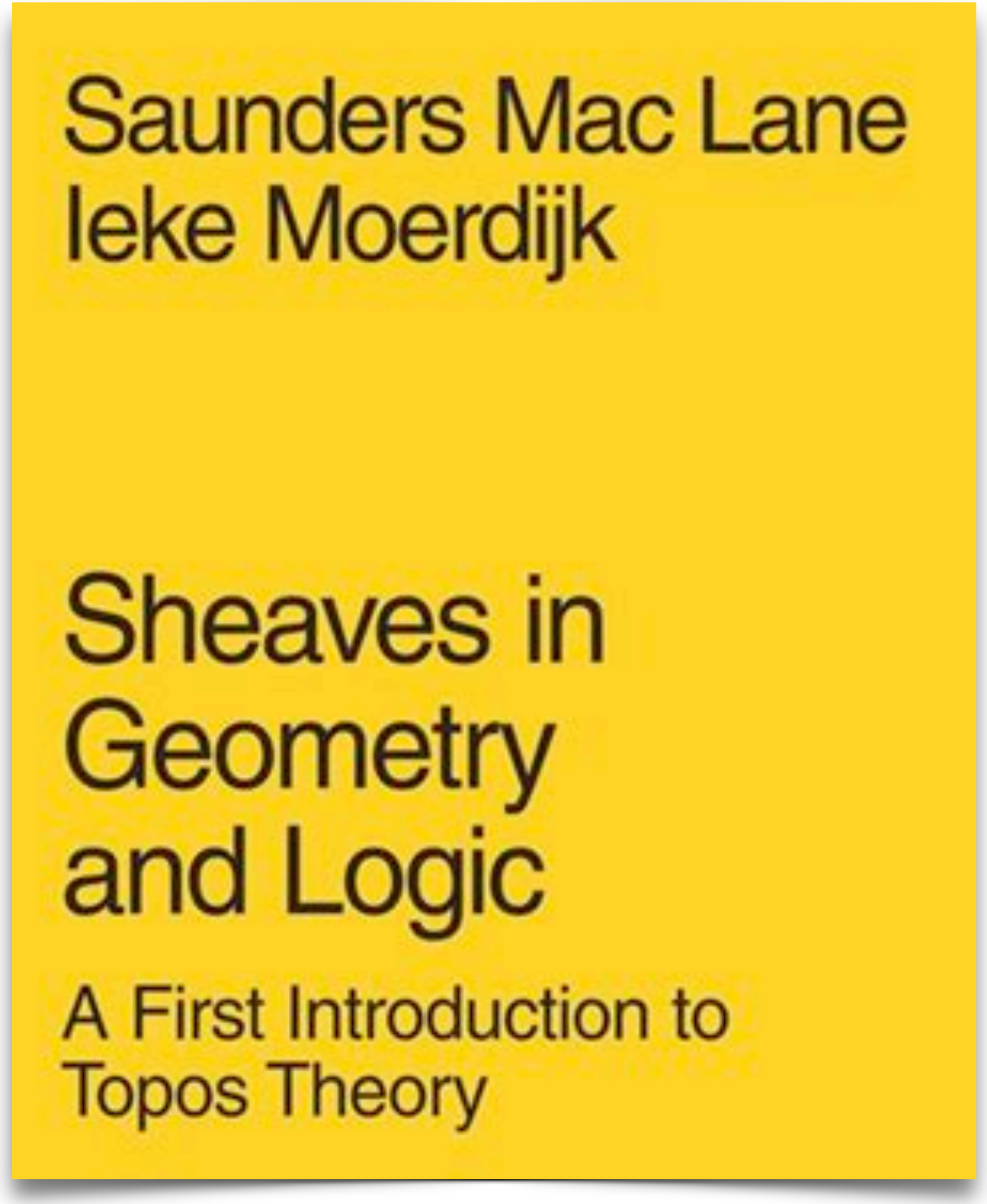
- Q: What does Day convolution have to do with disjoint union?

First, some history...

- Q: What does Day convolution have to do with disjoint union?
- A: It **is** disjoint union... up to a suitable equivalence of categories

First, some history...

- Q: What does Day convolution have to do with disjoint union?
- A: It **is** disjoint union... up to a suitable equivalence of categories

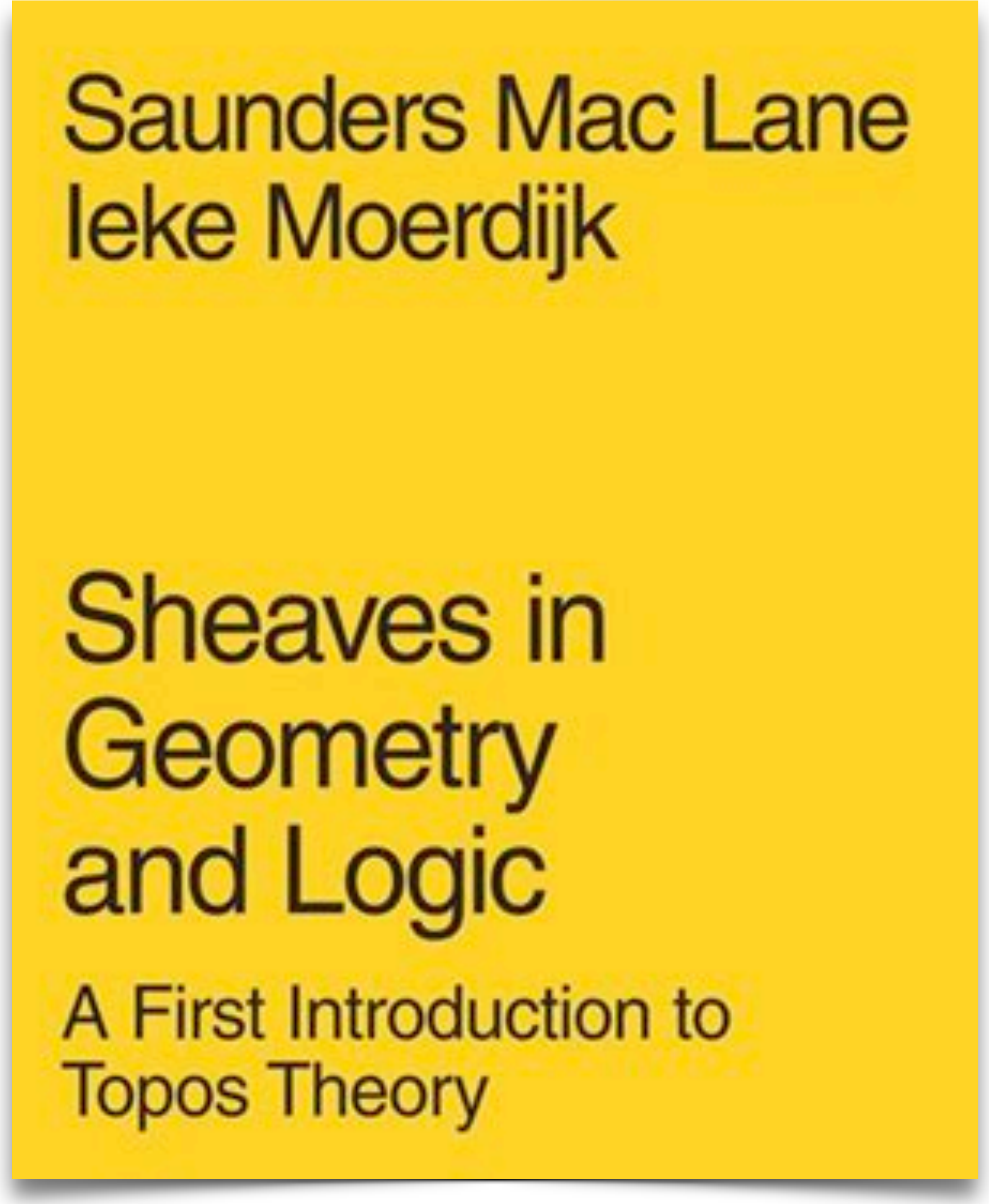


, Theorem III.9.2: $\mathbf{Sch} \simeq \mathbf{Nom}$.

First, some history...

- Q: What does Day convolution have to do with disjoint union?
- A: It **is** disjoint union... up to a suitable equivalence of categories

the category of nominal sets



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

First, some history...

- Q: What does Day convolution have to do with disjoint union?
- A: It **is** disjoint union... up to a suitable equivalence of categories
- Across this equivalence,

Day conv. w.r.t. coproduct in **Sch**	$\simeq$	pairs of disjoint heaps in **Nom**

Back to the present day

Back to the present day

- Q: Why isn't separation just about product spaces?
- A: It **is** just about product spaces... up to a suitable equivalence of categories

Back to the present day

- Q: Why isn't separation just about product spaces?
- A: It **is** just about product spaces... up to a suitable equivalence of categories

ProbSch

A "probabilistic Schanuel topos"

Back to the present day

- Q: Why isn't separation just about product spaces?
- A: It **is** just about product spaces... up to a suitable equivalence of categories

ProbSch

A "probabilistic Schanuel topos"

ProbNom

"Probabilistic nominal sets"

Back to the present day

- Q: Why isn't separation just about product spaces?
- A: It **is** just about product spaces... up to a suitable equivalence of categories

$$\mathbf{ProbSch} \simeq \mathbf{ProbNom}$$

ProbSch: A "probabilistic Schanuel topos"

ProbNom: "Probabilistic nominal sets"

Back to the present day

- Q: Why isn't separation just about product spaces?
- A: It **is** just about product spaces... up to a suitable equivalence of categories

- Across this equivalence,

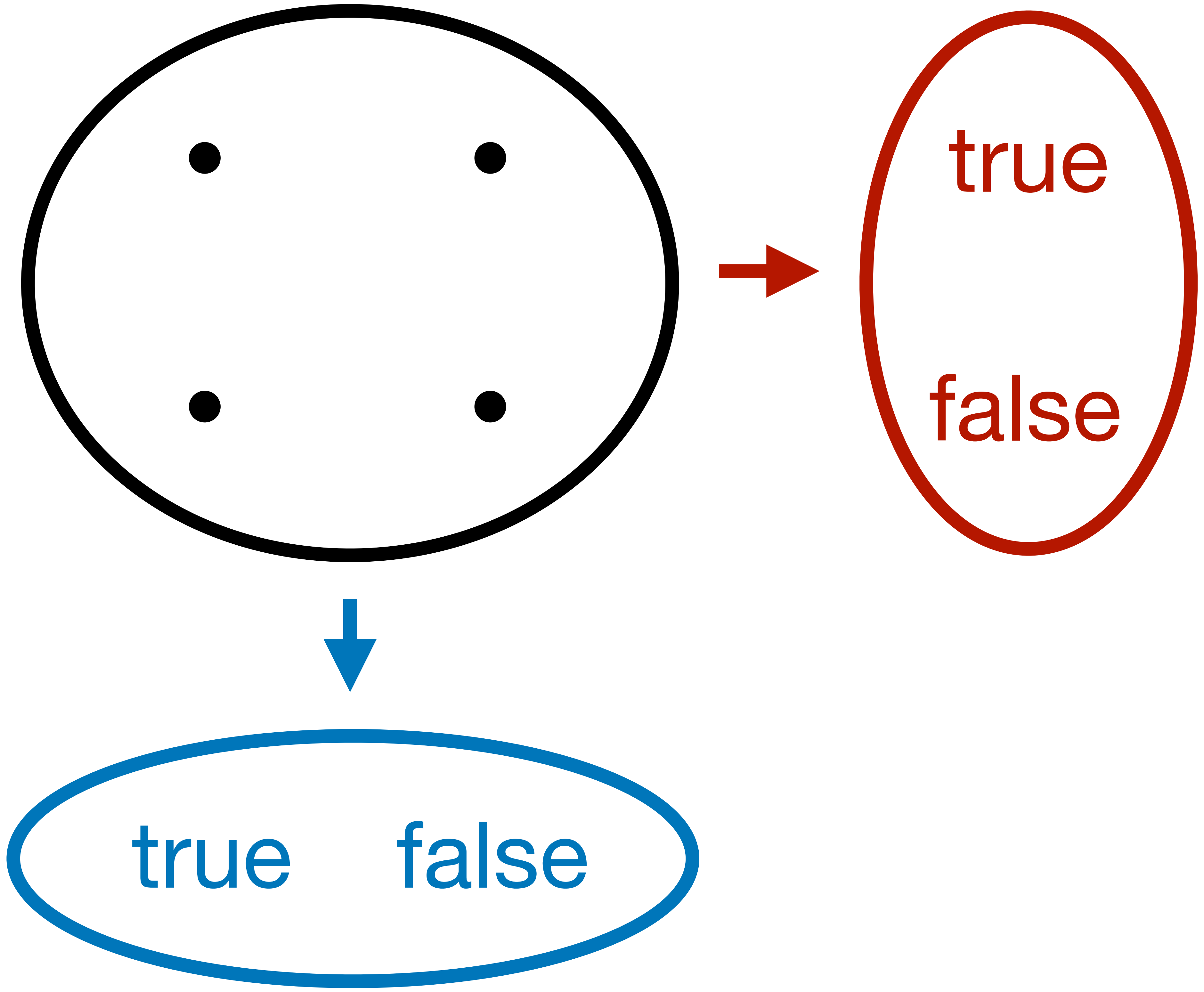
$$\begin{array}{ccc} \text{Day conv. w.r.t. product} & & \text{independent combination} \\ \text{in} & \simeq & \text{in} \\ \textbf{ProbSch} & & \textbf{ProbNom} \end{array}$$

Upshot

- The naive picture is right (with enough category theory):

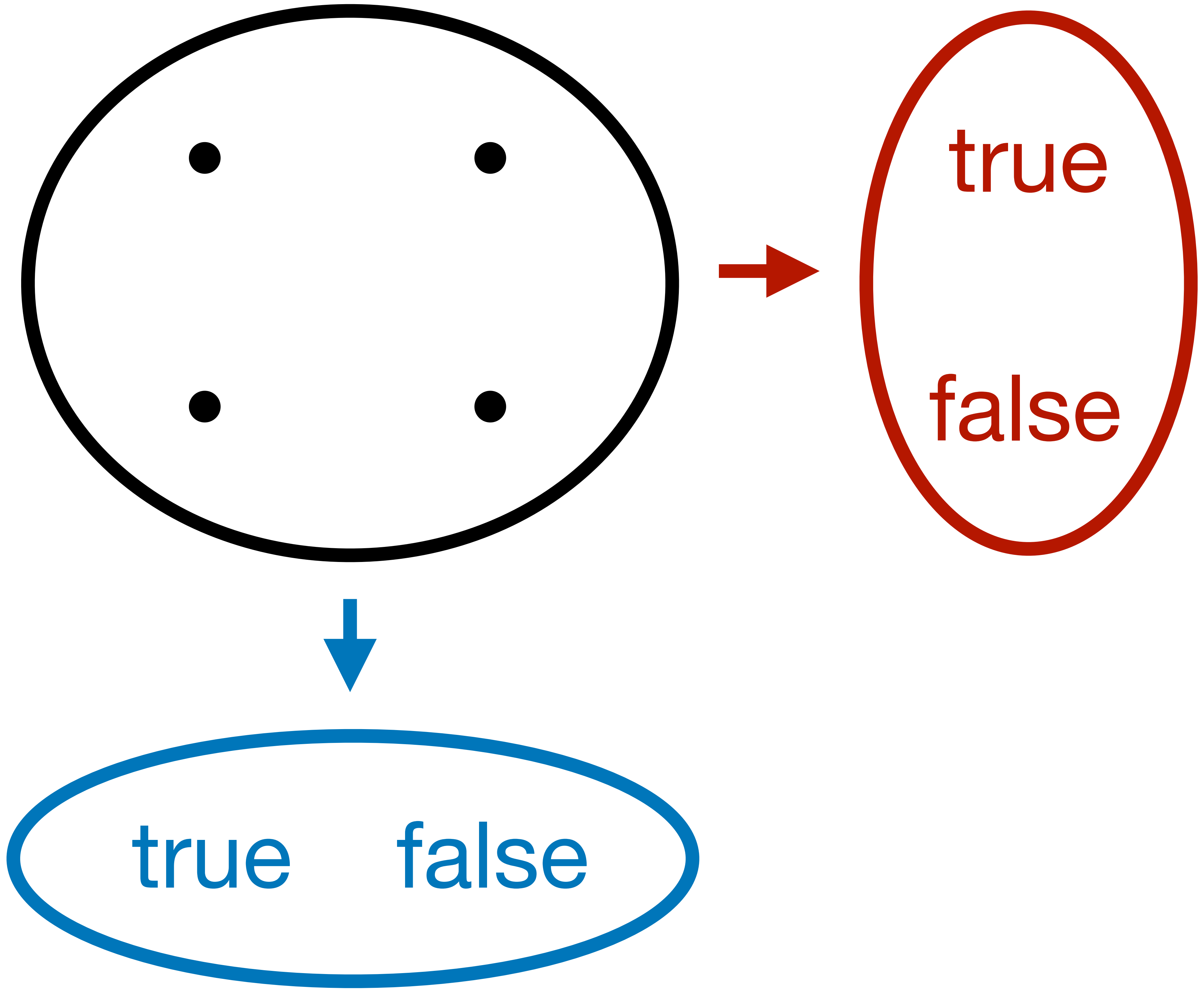
Upshot

- The naive picture is right (with enough category theory):



Upshot

- The naive picture is right (with enough category theory):



- And independent combination is right too!

Upshot

- Corroborates recent work linking probability to names

Upshot

- Corroborates recent work linking 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

Probability Sheaves and the Giry Monad*

Alex Simpson

Faculty of Mathematics and Physics, University of Ljubljana, Slovenia
Alex.Simpson@fmf.uni-lj.si

Upshot

- Corroborates recent work linking probability to names
- New nominal interpretations of probabilistic concepts:

Upshot

- Corroborates recent work linking probability to names
- New nominal interpretations of probabilistic concepts:

Probability theory		**Nominal sets**
Measurable space	$\sim$	Support
Measurability	$\sim$	Supportedness
Probability space	$\sim$	Store
Probabilistic independence	$\sim$	Disjointness of stores

Upshot

https://johnm.li/lafi24.pdf

- Corroborates recent work linking probability to names
- New nominal interpretations of probabilistic concepts:

Probability theory		Nominal sets
Measurable space	$\sim$	Support
Measurability	$\sim$	Supportedness
Probability space	$\sim$	Store
Probabilistic independence	$\sim$	Disjointness of stores

- ==> maybe nominal techniques apply to probability?