Lilac: A Modal Separation Logic for Conditional Probability

John Li
li.john@northeastern.edu

Amal Ahmed
amal@ccs.neu.edu

Steven Holtzen
s.holtzen@northeastern.edu

Northeastern University
Khoury College of Computer Sciences

https://johnm.li/lilac.pdf

How to reason about complex probabilistic systems?

How to reason about complex probabilistic systems?

How to reason about complex probabilistic systems?

How to reason about complex probabilistic systems?

How to reason about complex probabilistic systems?

Is my car safe?

How to reason about complex probabilistic systems?

Is my car safe?

Is this decision fair?

How to reason about complex probabilistic systems?

Is my car safe?

Is this decision fair?

Is my result significant?

How to reason about complex probabilistic systems?

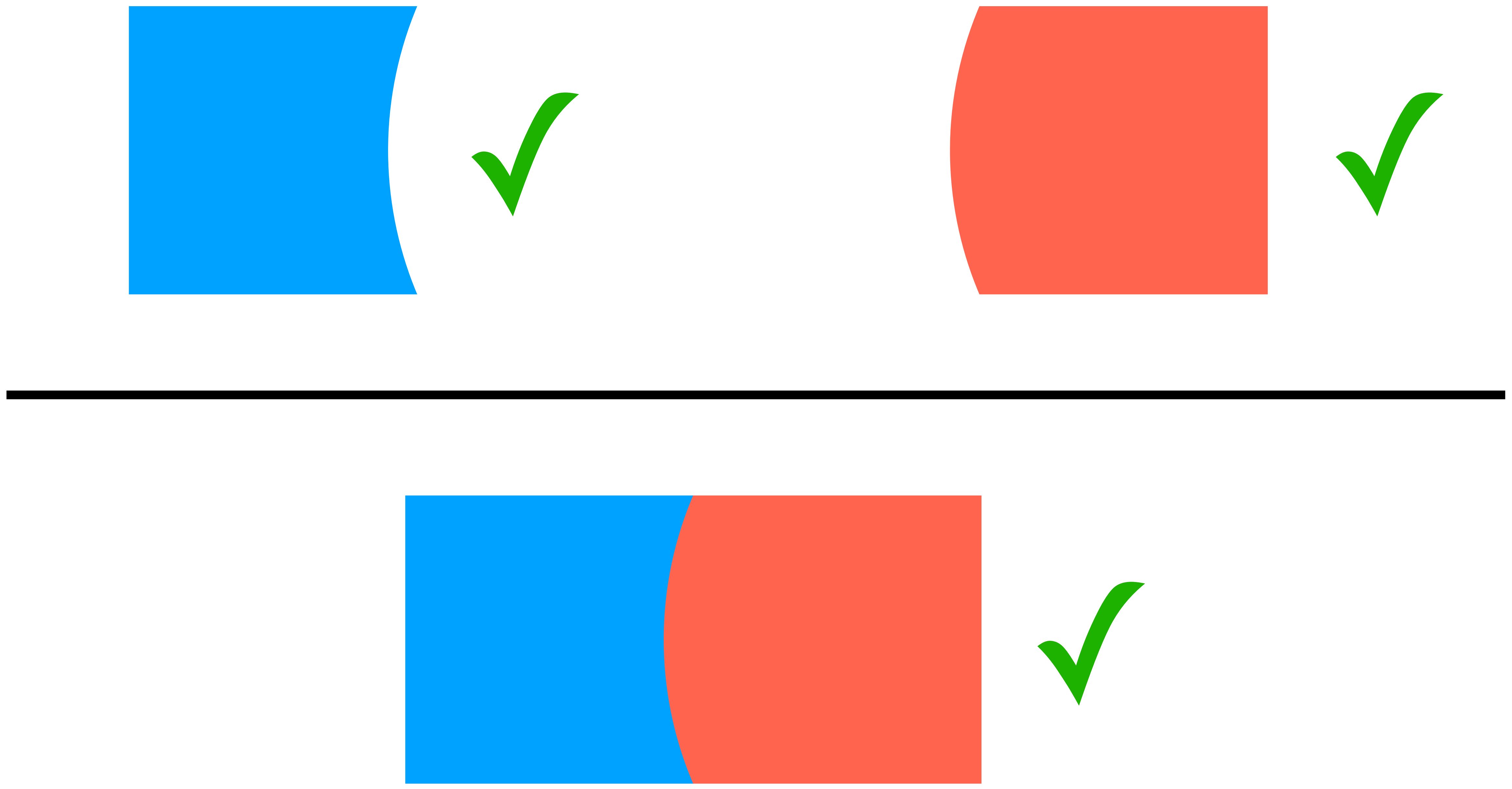
- Reasoning should be *modular*:

How to reason about complex probabilistic systems?

- Reasoning should be *modular*:

How to reason about complex probabilistic systems?

- Reasoning should be *modular*:



Modularity comes from probabilistic independence

- Independence arises frequently and naturally:

Modularity comes from probabilistic independence

- Independence arises frequently and naturally:

$$\texttt{weights} = \texttt{np.random.rand}(1000)$$

Modularity comes from probabilistic independence

- Independence arises frequently and naturally:

$$\texttt{weights} = \texttt{np.random.rand}(1000)$$

$\texttt{weights}[0], \ldots, \texttt{weights}[999] \sim \text{Unif}[0,1]$ mutually independent

Modularity comes from probabilistic independence

- Independence arises frequently and naturally:

$$\mathtt{result} = \mathtt{np.mean}(\mathtt{data})$$

Modularity comes from probabilistic independence

- Independence arises frequently and naturally:

if each `data[i]` is an independent estimate of v...

```
result = np.mean(data)
```

...then `result` is a more accurate estimate of v

Modularity comes from probabilistic independence

- Independence arises frequently and naturally.
- Idea: capture independence using *separation logic*

Ordinary separation logic is about disjointness

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

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

Ordinary separation logic is about disjointness

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

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

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

Ordinary separation logic is about disjointness

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

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

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

↑

x and y point to disjoint heap locations

Ordinary separation logic is about disjointness

$$\frac{\{P\}\ e\ \{x\,.\,Q(x)\}}{\{P * F\}\ e\ \{x\,.\,Q(x) * F\}}\ \text{(Frame)}$$

Ordinary separation logic is about disjointness

When verifying e...

$$\frac{\{P\}\ e\ \{x\,.\,Q(x)\}}{\{P * F\}\ e\ \{x\,.\,Q(x) * F\}}\ \text{(Frame)}$$

Ordinary separation logic is about disjointness

When verifying e...

...I can ignore disjoint subheaps F

$$\frac{\{P\}\ e\ \{x\,.\,Q(x)\}}{\{P * F\}\ e\ \{x\,.\,Q(x) * F\}}\ \text{(Frame)}$$

Ordinary separation logic is about disjointness

When verifying e...

...I can ignore disjoint subheaps F

$$\frac{\{P\}\ e\ \{x\,.\,Q(x)\}}{\{P * F\}\ e\ \{x\,.\,Q(x) * F\}}\ \text{(Frame)}$$

- This has enabled modular heap-based reasoning at scale.[1]

[1] C. Calcagno and D. Distefano. Infer: An automatic program verifier for memory safety of C programs. NFM 2011.

Lilac's separation is about independence

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

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

Lilac's separation is about independence

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

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

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

Lilac's separation is about independence

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

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

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

↑

X and Y are independent random variables

Wait, hasn't this been done before?

Wait, hasn't this been done before?

A Probabilistic Separation Logic

GILLES BARTHE, MPI for Security and Privacy, Germany and IMDEA Software Institute, Spain
JUSTIN HSU, University of Wisconsin–Madison, USA
KEVIN LIAO, MPI for Security and Privacy, Germany and University of Illinois Urbana-Champaign, USA

POPL'20

New in Lilac

New in Lilac: a simple frame rule

New in Lilac: a simple frame rule

$$\frac{\{P\}\ e\ \{x\,.\,Q(x)\}}{\{P * F\}\ e\ \{x\,.\,Q(x) * F\}}\ \text{(Frame)}$$

New in Lilac: a simple frame rule

$$\frac{\{P\}\ e\ \{x\,.\,Q(x)\}}{\{P * F\}\ e\ \{x\,.\,Q(x) * F\}}\ \text{(Frame)}$$

- Just like in ordinary separation logic!

New in Lilac: separation is independence

New in Lilac: separation is independence

$$\texttt{weights} = \texttt{np.random.rand}(1000)$$

$\texttt{weights}[0], \ldots, \texttt{weights}[999] \sim \mathrm{Unif}[0,1]$ mutually independent

New in Lilac: separation is independence

$$\texttt{weights} = \texttt{np.random.rand}(1000)$$

$$(\texttt{weights}[0] \sim \mathrm{Unif}[0,1]) \ast \cdots \ast (\texttt{weights}[999] \sim \mathrm{Unif}[0,1])$$

New in Lilac: separation is independence

$$\texttt{weights} = \texttt{np.random.rand}(1000)$$

$$(\texttt{weights}[0] \sim \text{Unif}[0,1]) \; * \; \cdots \; * \; (\texttt{weights}[999] \sim \text{Unif}[0,1])$$

Inexpressible in PSL

New in Lilac: separation is independence

$$\texttt{weights} = \texttt{np.random.rand}(1000)$$

$$(\texttt{weights}[0] \sim \mathrm{Unif}[0,1]) \ast \cdots \ast (\texttt{weights}[999] \sim \mathrm{Unif}[0,1])$$

Completely captures independence (Lemma 2.5)

New in Lilac: quantitative reasoning

New in Lilac: quantitative reasoning

if each `data[i]` is an independent estimate of v...

$$\texttt{result} = \texttt{np.mean(data)}$$

...then `result` is a more accurate estimate of v

New in Lilac: quantitative reasoning

if each `data[i]` independent
and for all i we have $\mathbb{E}[\texttt{data[i]}] = v$ and $\mathrm{Var}(\texttt{data[i]}) \leq \varepsilon$...

$$\texttt{result} = \texttt{np.mean(data)}$$

...then `result` is a more accurate estimate of v

New in Lilac: quantitative reasoning

if each `data[i]` independent
and for all i we have $\mathbb{E}[\mathtt{data[i]}] = v$ and $\mathrm{Var}(\mathtt{data[i]}) \leq \varepsilon$...

$$\mathtt{result} = \mathtt{np.mean}(\mathtt{data})$$

...then $\mathbb{E}[\mathtt{result}] = v$ and $\mathrm{Var}(\mathtt{result}) \leq \dfrac{\varepsilon}{|\mathtt{data}|}$

New in Lilac: quantitative reasoning

if $\underset{0 \leq i < |\mathtt{data}|}{\circledast} \left(\mathbb{E}[\mathtt{data[i]}] = v \text{ and } \mathrm{Var}(\mathtt{data[i]}) \leq \varepsilon \right)$...

$$\mathtt{result = np.mean(data)}$$

...then $\mathbb{E}[\mathtt{result}] = v$ and $\mathrm{Var}(\mathtt{result}) \leq \dfrac{\varepsilon}{|\mathtt{data}|}$

New in Lilac: good interop with normal math

$$\text{if} \quad \mathop{\Huge\ast}_{0 \le i < |\texttt{data}|} \left(\mathbb{E}[\texttt{data[i]}] = \nu \text{ and } \mathrm{Var}(\texttt{data[i]}) \le \varepsilon \right) \ldots$$

$$\texttt{result} = \texttt{np.mean(data)}$$

$$\ldots\text{then } \mathbb{E}[\texttt{result}] = \nu \text{ and } \mathrm{Var}(\texttt{result}) \le \frac{\varepsilon}{|\texttt{data}|}$$

New in Lilac: good interop with normal math

if $\mathop{\circledast}\limits_{0 \le i < |\mathtt{data}|} \left(\mathbb{E}[\mathtt{data[i]}] = v \text{ and } \mathrm{Var}(\mathtt{data[i]}) \le \varepsilon \right)$...

$$\mathtt{result} = \mathtt{np.mean(data)}$$

...then $\mathbb{E}[\mathtt{result}] = v$ and $\mathrm{Var}(\mathtt{result}) \le \dfrac{\varepsilon}{|\mathtt{data}|}$

An ordinary random variable

New in Lilac: good interop with normal math

if $\underset{0 \leq i < |\texttt{data}|}{\circledast} \left(\mathbb{E}[\texttt{data[i]}] = v \text{ and } \mathrm{Var}(\texttt{data[i]}) \leq \varepsilon \right)$...

$$\texttt{result} = \texttt{np.mean(data)}$$

...then $\mathbb{E}[\texttt{result}] = v$ and $\mathrm{Var}(\texttt{result}) \leq \dfrac{\varepsilon}{|\texttt{data}|}$

Ordinary expectation and variance

New in Lilac: good interop with normal math

if $\underset{0 \le i < |\mathtt{data}|}{\circledast} \left(\mathbb{E}[\mathtt{data[i]}] = v \text{ and } \mathrm{Var}(\mathtt{data[i]}) \le \varepsilon \right)$...

$$\mathtt{result} = \mathtt{np.mean(data)}$$

...then $\mathbb{E}[\mathtt{result}] = v$ and $\mathrm{Var}(\mathtt{result}) \le \dfrac{\varepsilon}{|\mathtt{data}|}$

$\implies$ textbook proofs remain textbook

Key idea

Key idea

- Probability spaces are the heaps of probability theory.

Probability spaces as heaps

Probability spaces as heaps

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

Probability spaces as heaps

$X \sim \mathrm{Ber}(1/2)$ means $\Pr[X = \mathrm{true}] = \Pr[X = \mathrm{false}] = 1/2$

Probability spaces as heaps

$X \sim \mathrm{Ber}(1/2)$ means $\Pr[X = \mathrm{true}] = \Pr[X = \mathrm{false}] = 1/2$

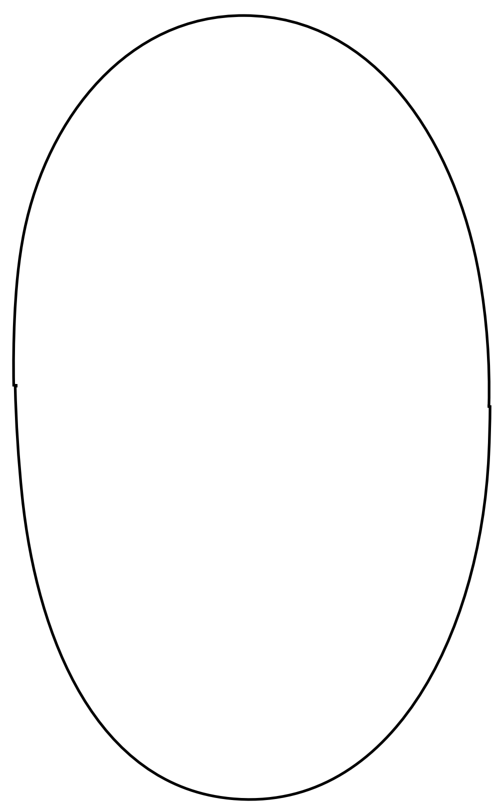
This hides a lot of machinery...

Probability spaces as heaps

$X \sim \mathrm{Ber}(1/2)$ really means...

Probability spaces as heaps

$X \sim \mathrm{Ber}(1/2)$ really means...

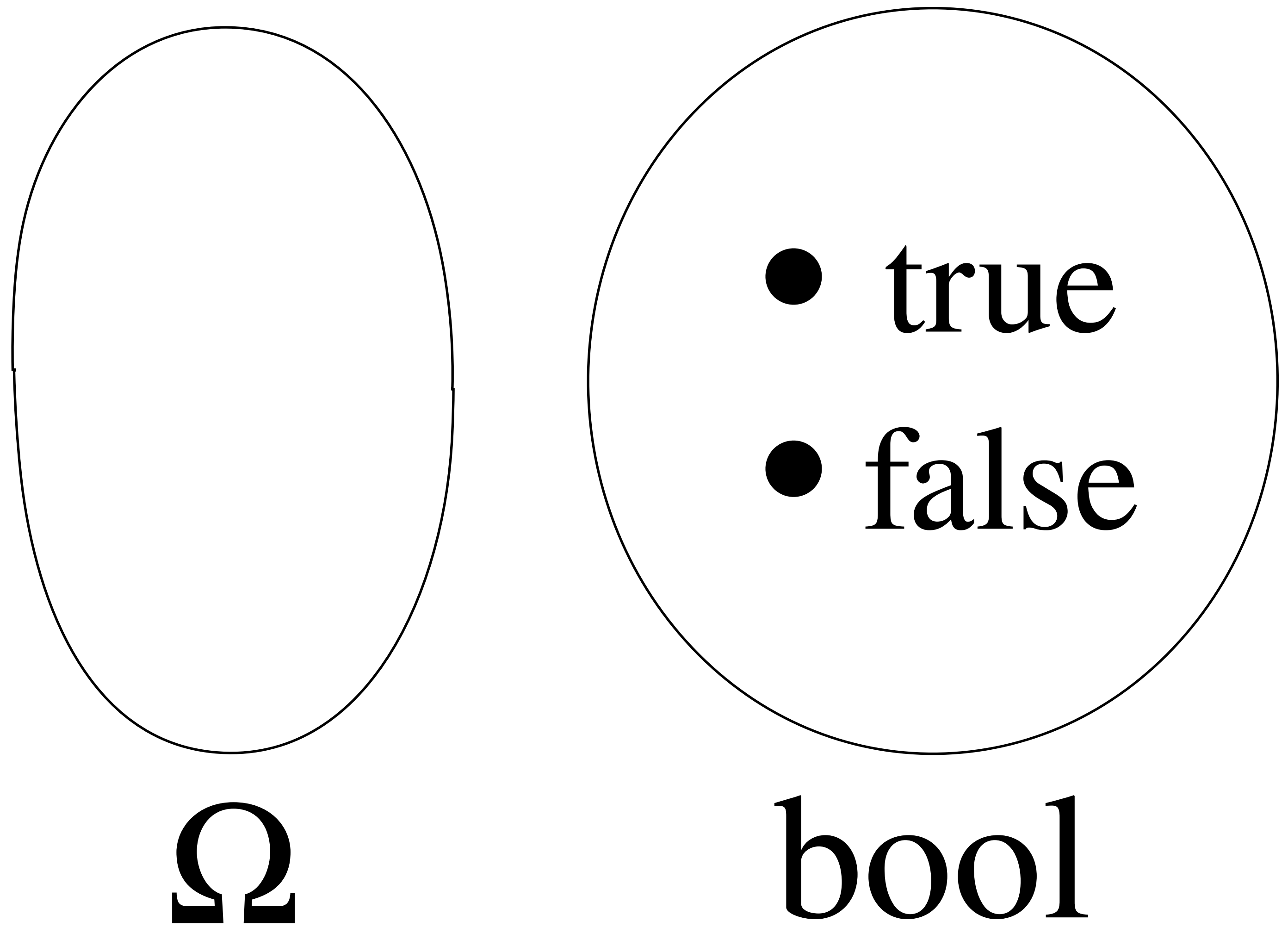


Ω

Probability spaces as heaps

$X \sim \mathrm{Ber}(1/2)$ really means...

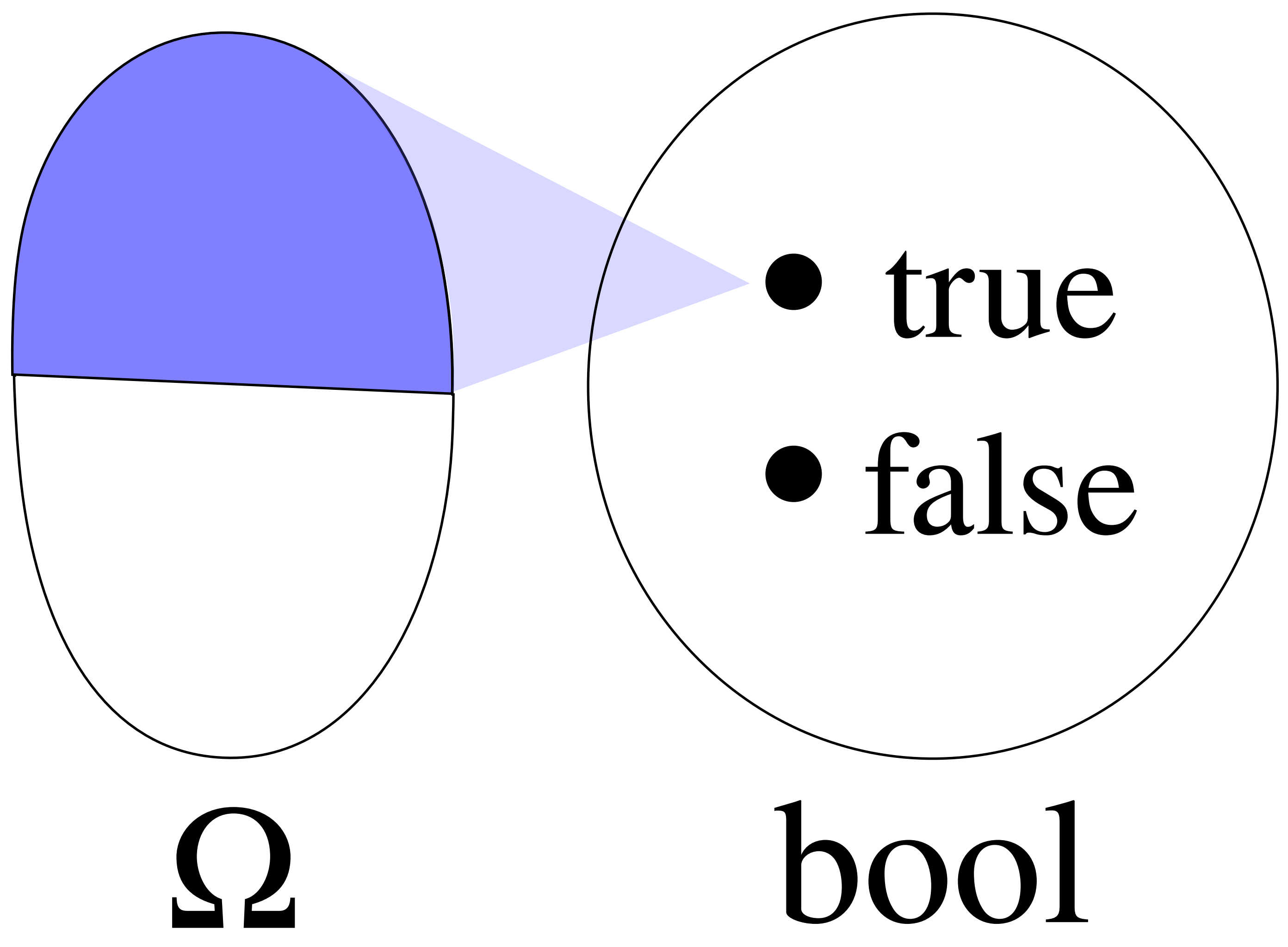
$$X : \Omega \rightarrow \mathrm{bool}$$



Probability spaces as heaps

$X \sim \mathrm{Ber}(1/2)$ really means...

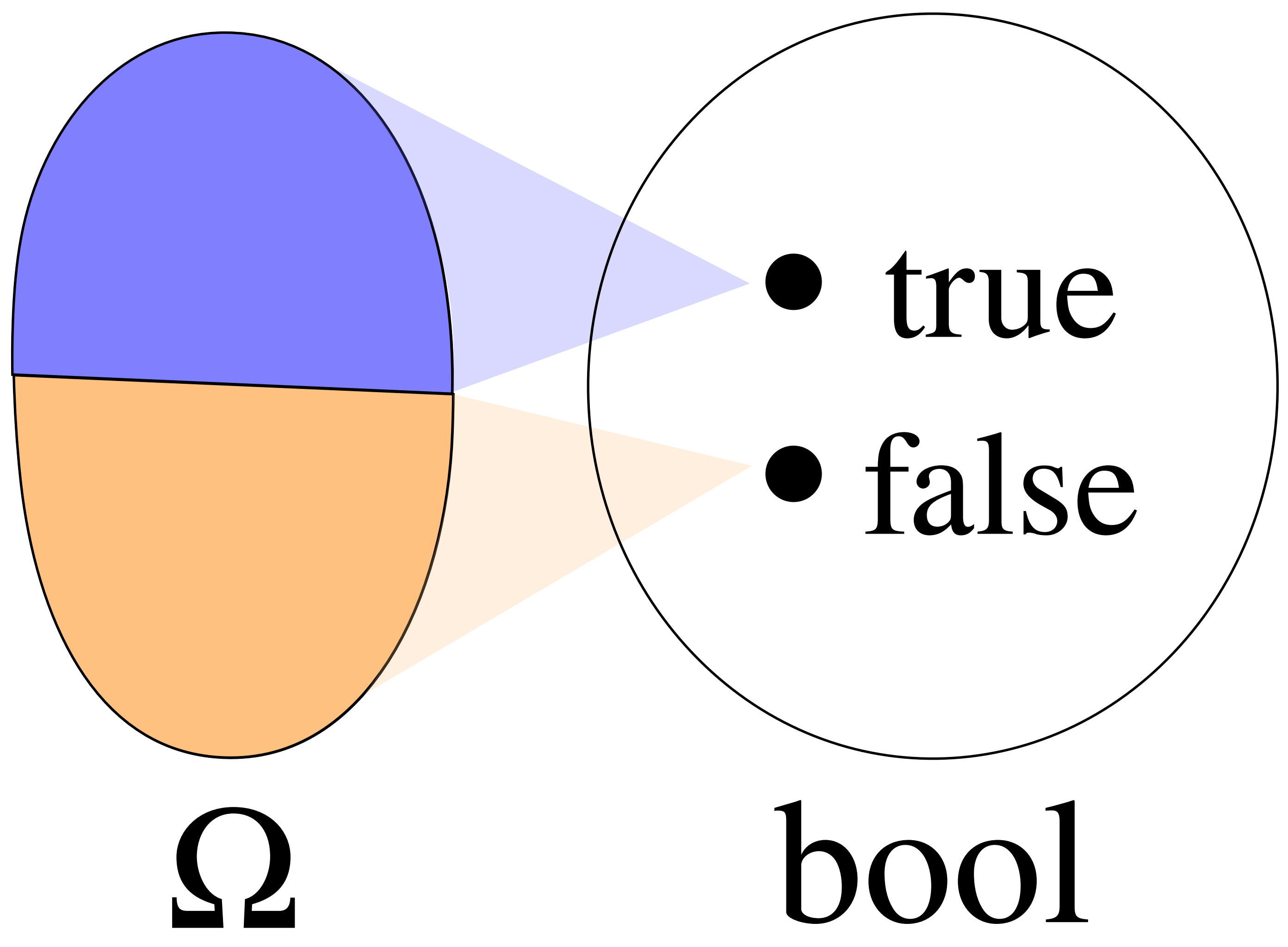
$X : \Omega \to \mathrm{bool}$



Probability spaces as heaps

$X \sim \mathrm{Ber}(1/2)$ really means...

$$X : \Omega \to \mathrm{bool}$$

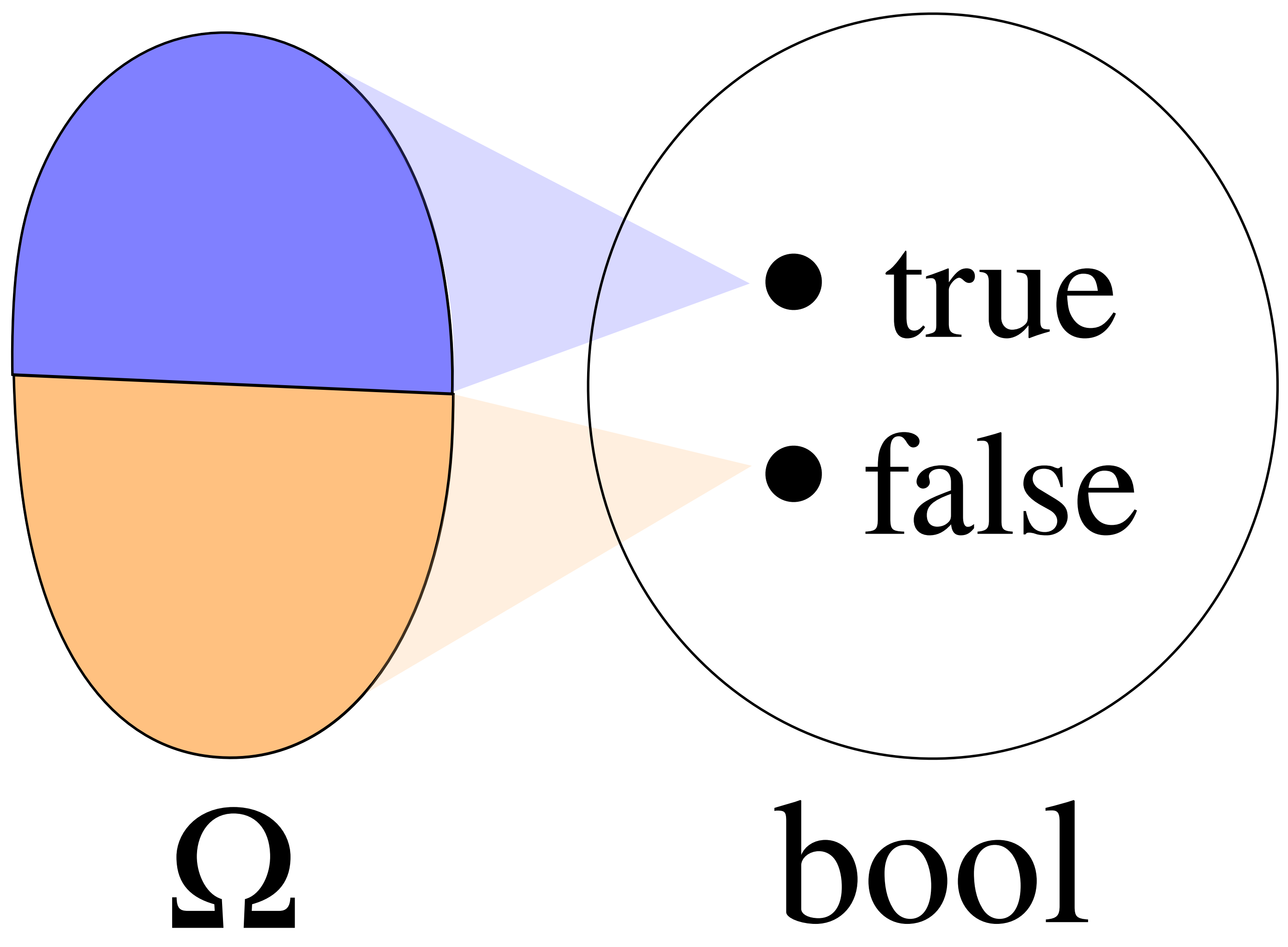


Probability spaces as heaps

$X \sim \mathrm{Ber}(1/2)$ really means...

$X : \Omega \to \mathrm{bool}$

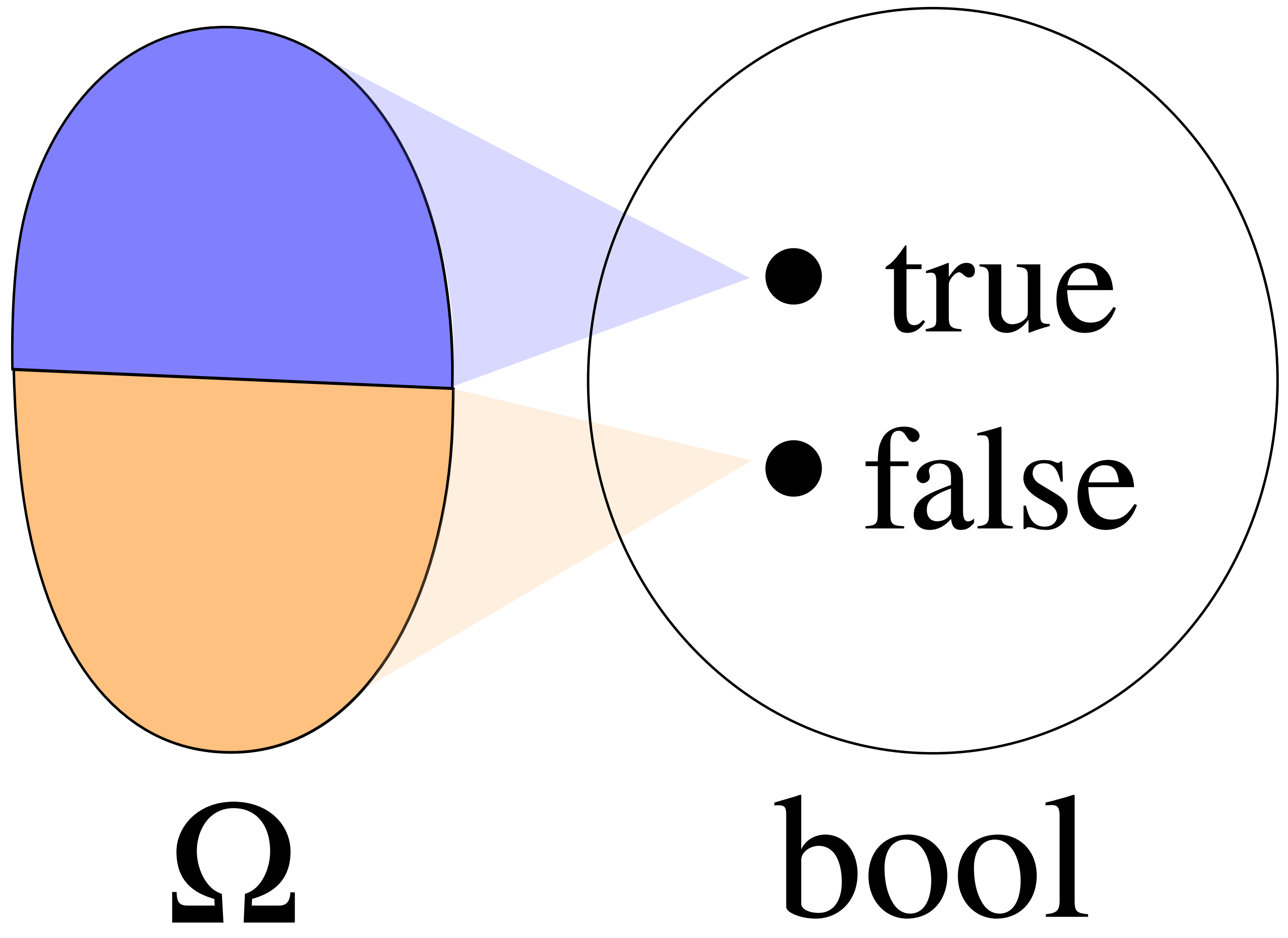
μ : events $\to [0,1]$



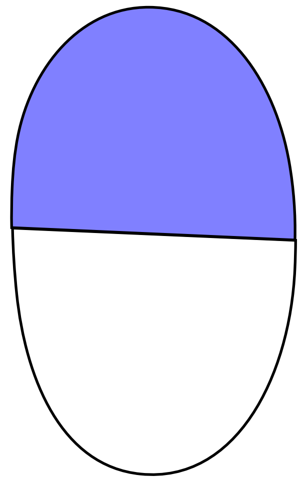
Probability spaces as heaps

$X \sim \text{Ber}(1/2)$ really means...

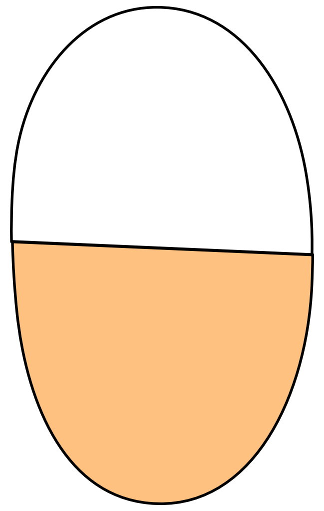
$X : \Omega \to \text{bool}$



μ : events $\to [0,1]$



$\in$ events

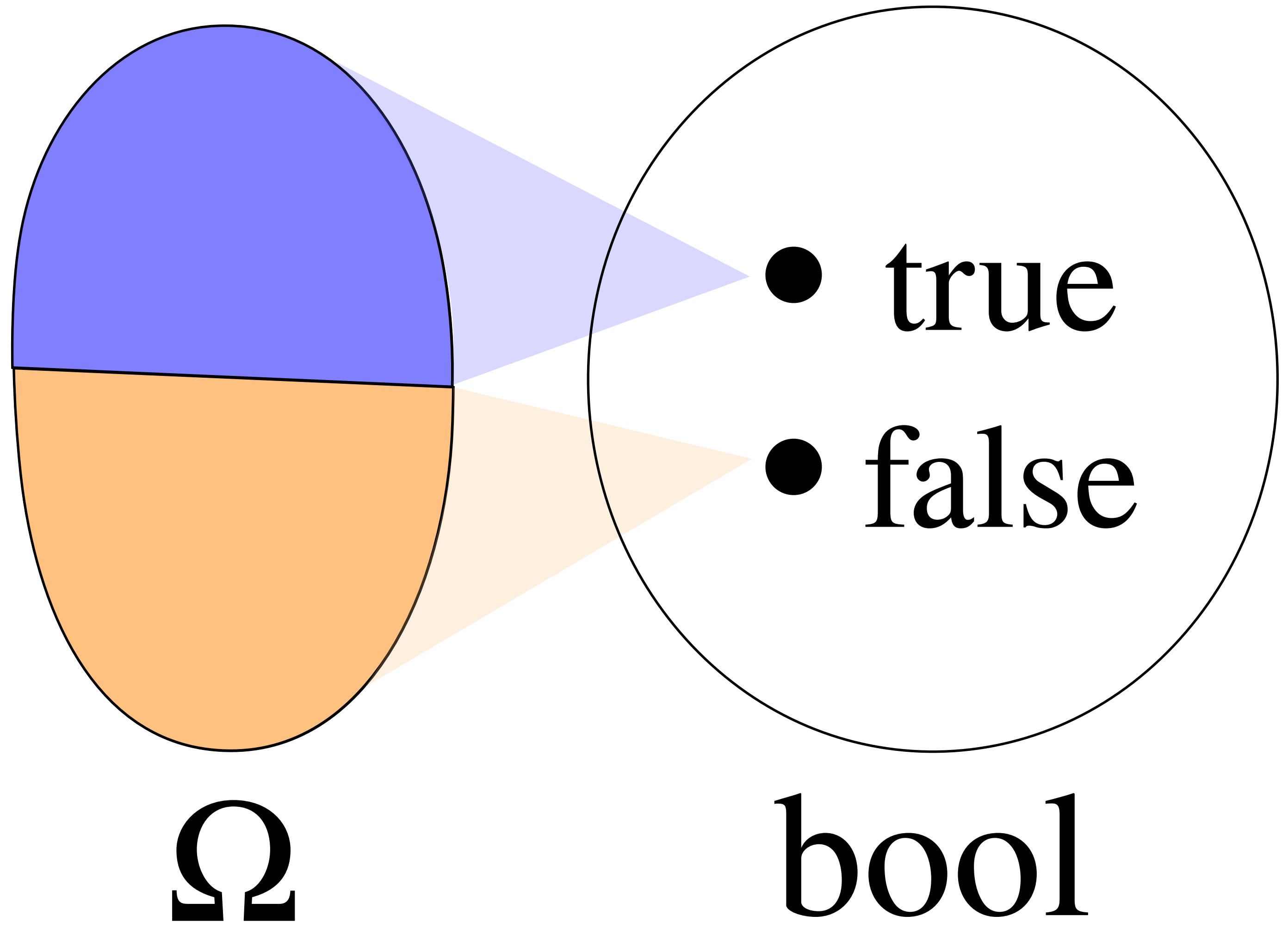


$\in$ events

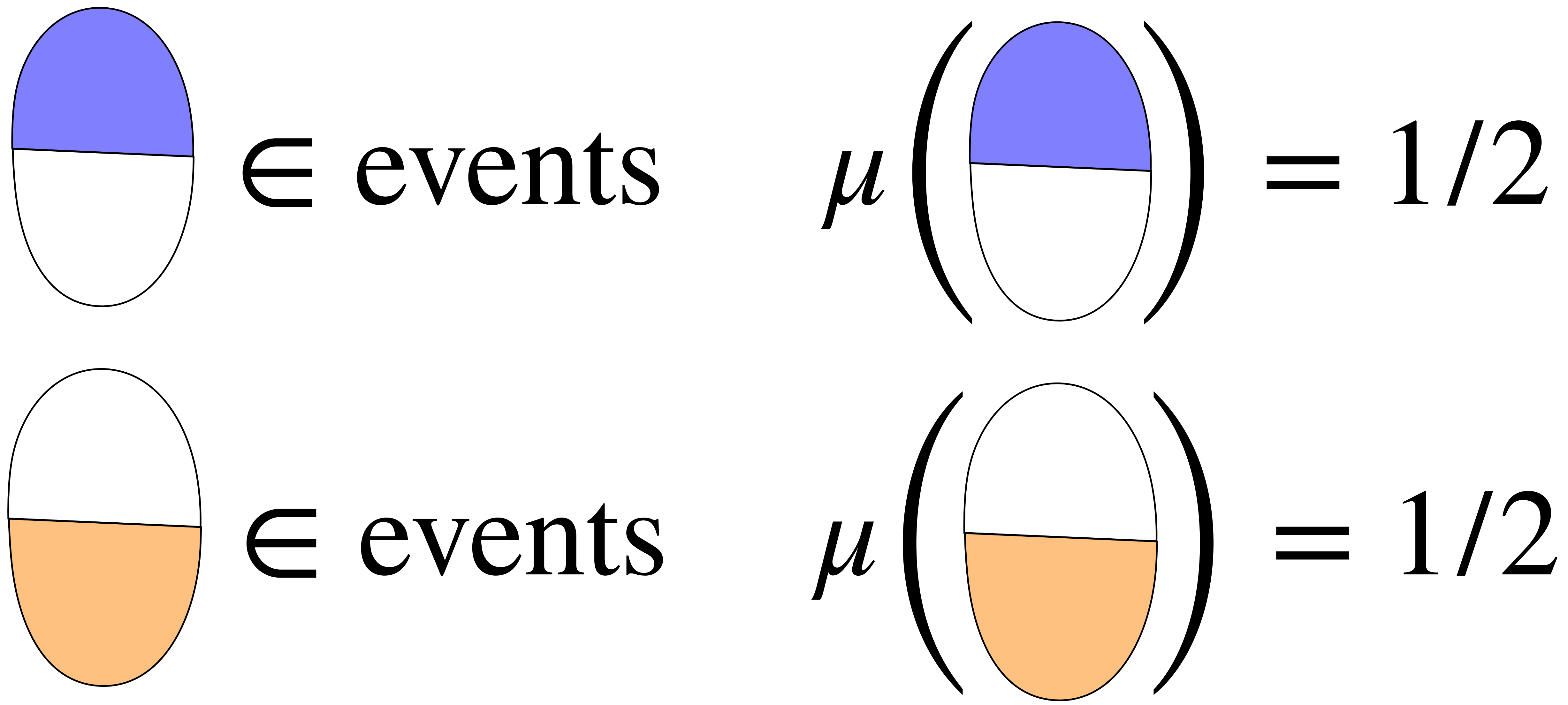
Probability spaces as heaps

$X \sim \mathrm{Ber}(1/2)$ really means...

$X : \Omega \to \mathrm{bool}$



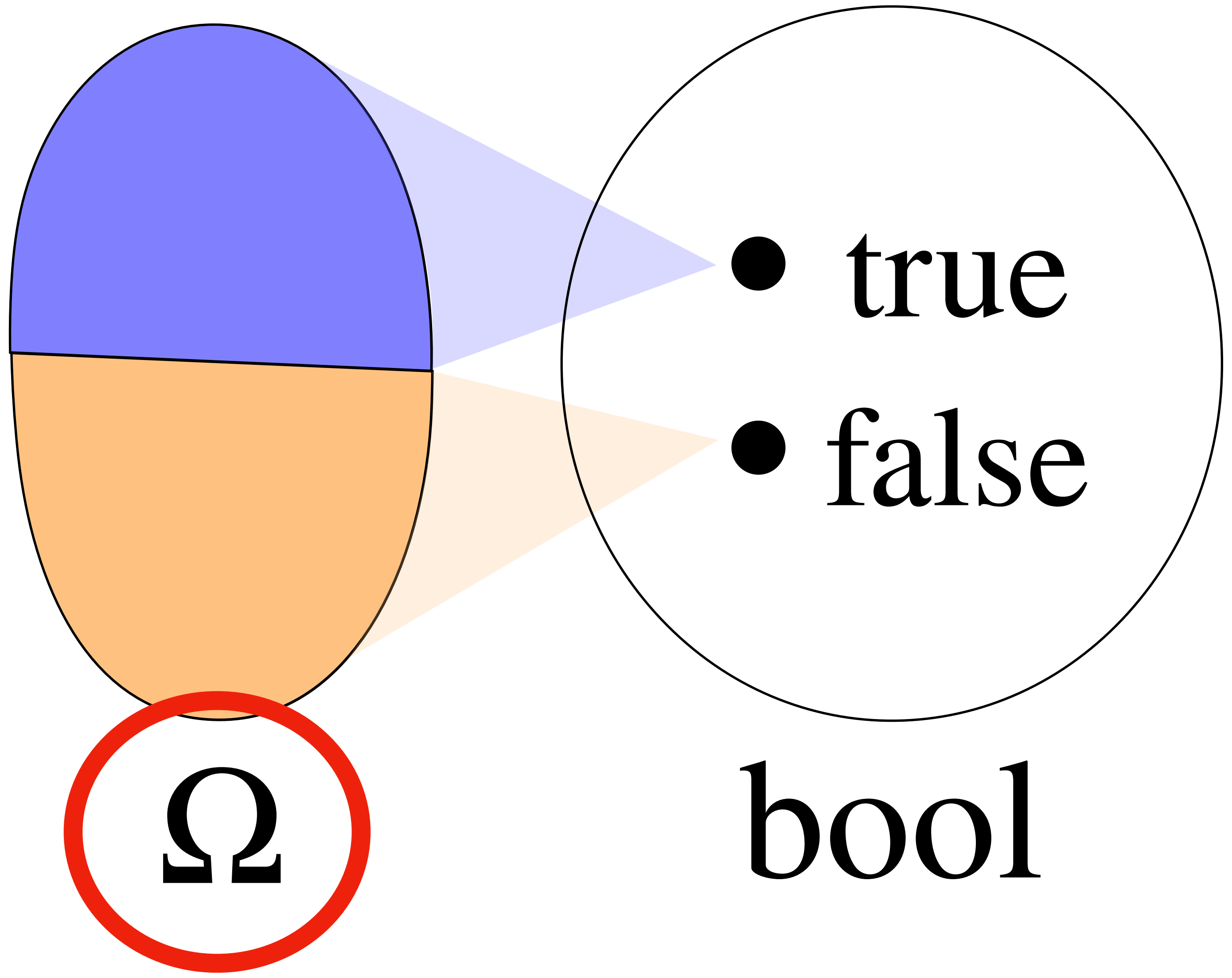
μ : events $\to [0,1]$



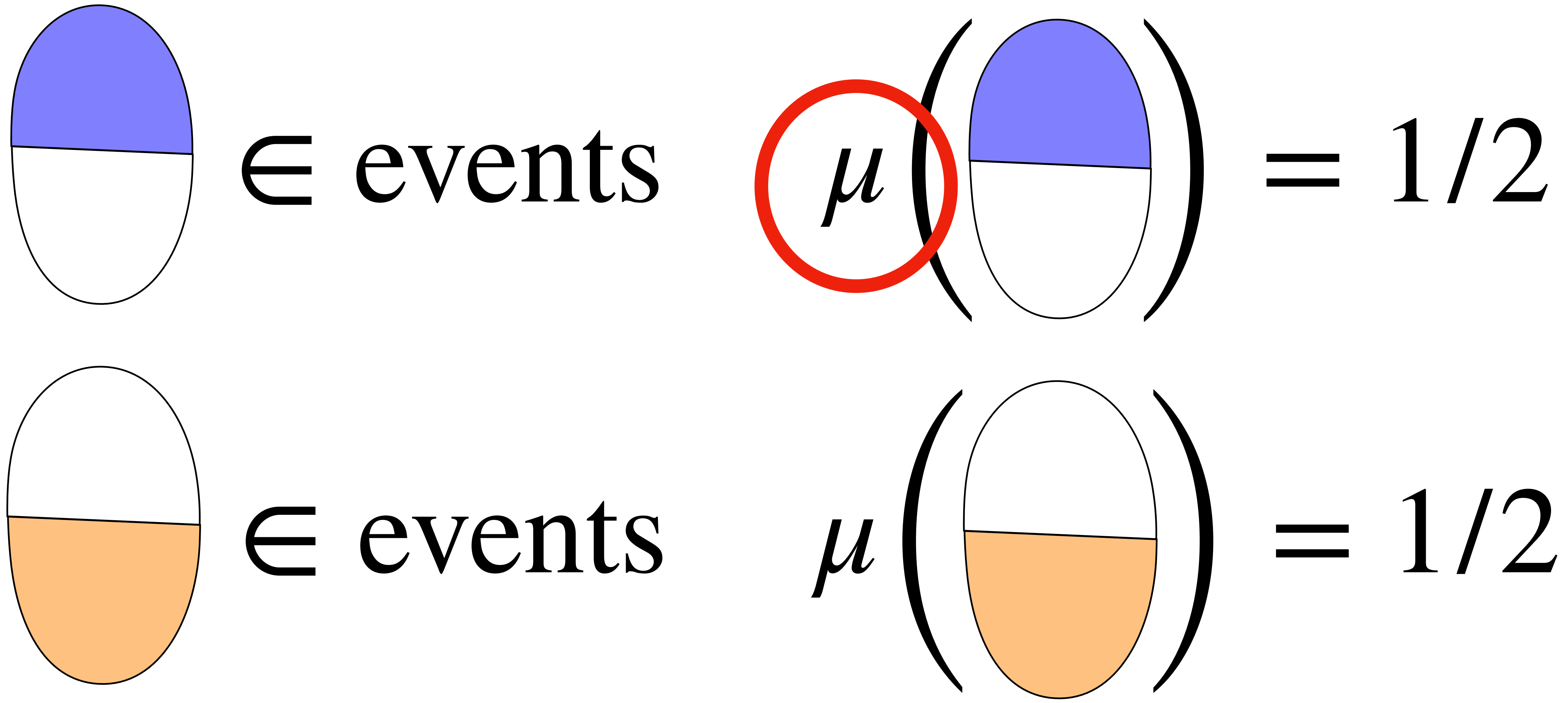
Probability spaces as heaps

$X \sim \mathrm{Ber}(1/2)$ really means...

$X : \Omega \to \mathrm{bool}$



$\mu : \mathrm{events} \to [0,1]$



Probability spaces as heaps

$X \sim \text{Ber}(1/2)$ really means...

events

μ

Ω

Probability spaces as heaps

$X \sim \mathrm{Ber}(1/2)$ really means...

events

Only accessed indirectly through X

μ

Ω

Probability spaces as heaps

$X \sim \mathrm{Ber}(1/2)$ really means...

events

Only accessed indirectly through X

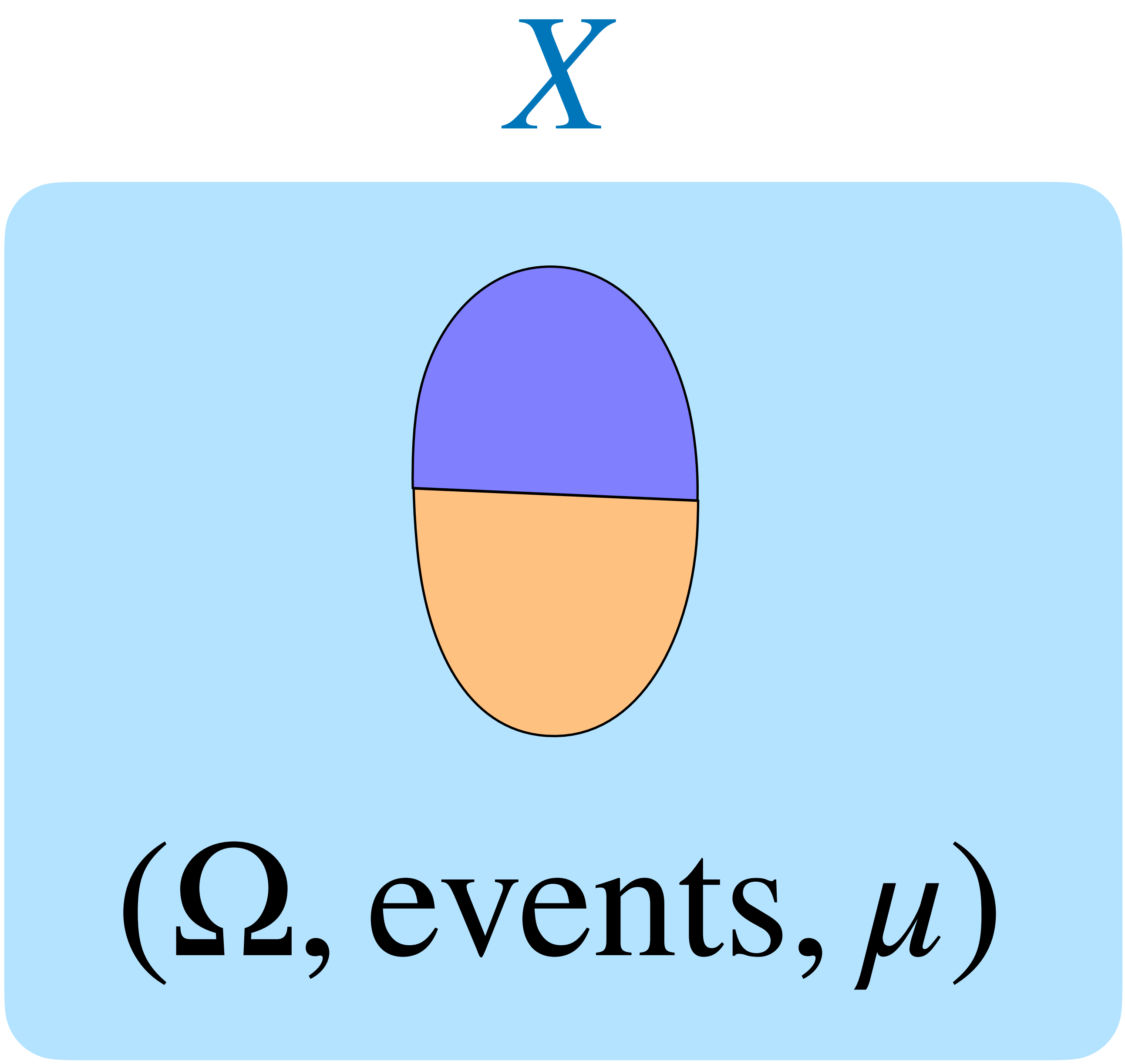
μ

Together, form a probability space

Ω

Probability spaces as heaps

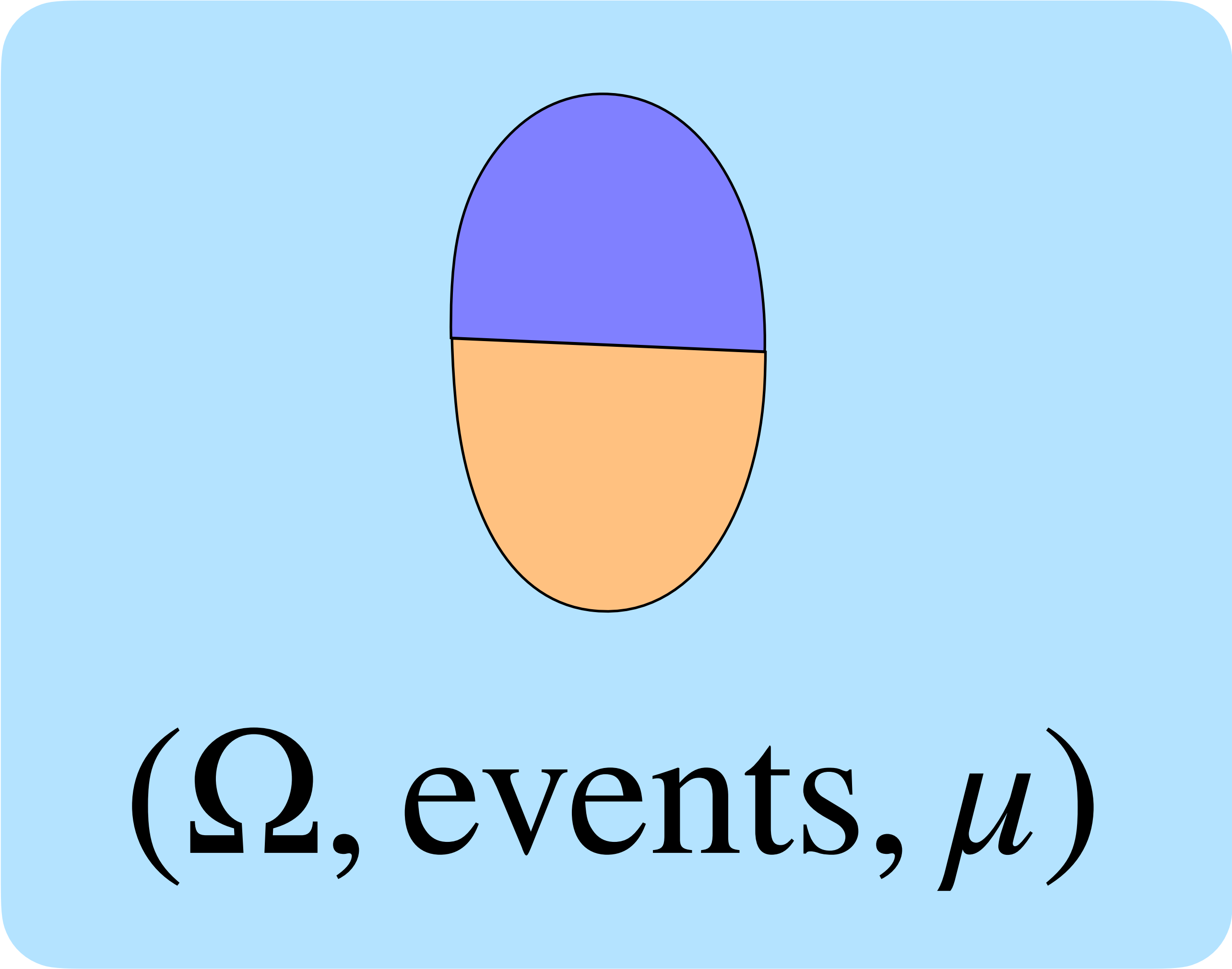
Probability theory



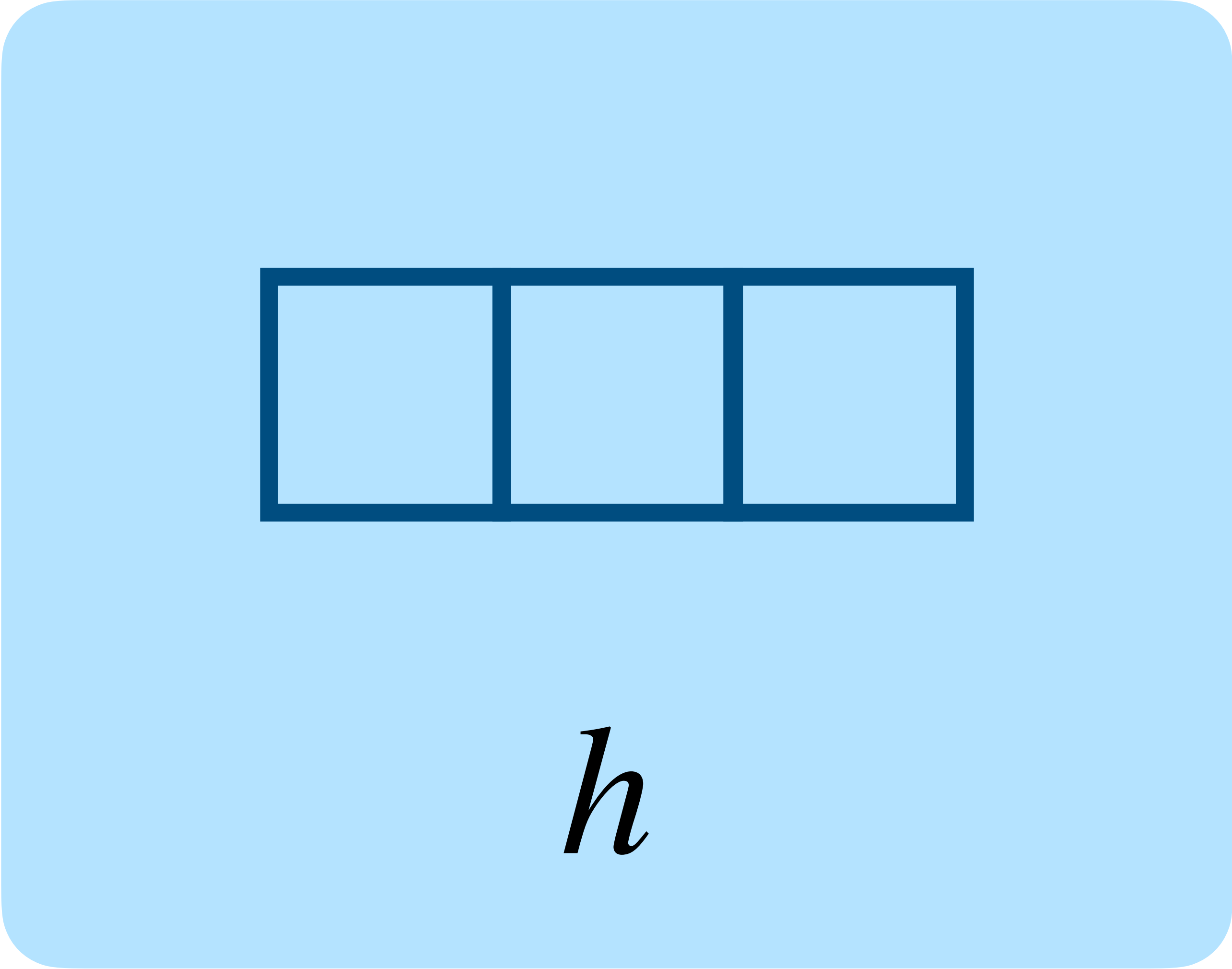
Probability spaces as heaps

Probability theory $\simeq$ Mutable references

X



ℓ



Key idea

- Probability spaces are the heaps of probability theory.

Key idea

- Probability spaces are the heaps of probability theory.

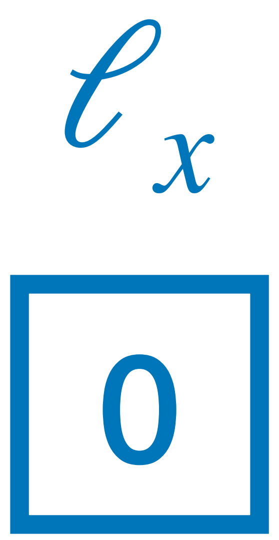
$x = \mathsf{new}\ 0;$

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

Key idea

- <u>Probability spaces are the heaps of probability theory.</u>

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

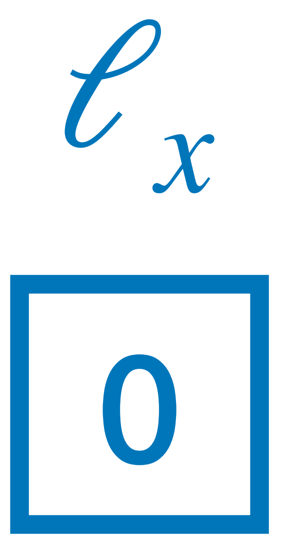


$y = \textsf{new}\ 1;$

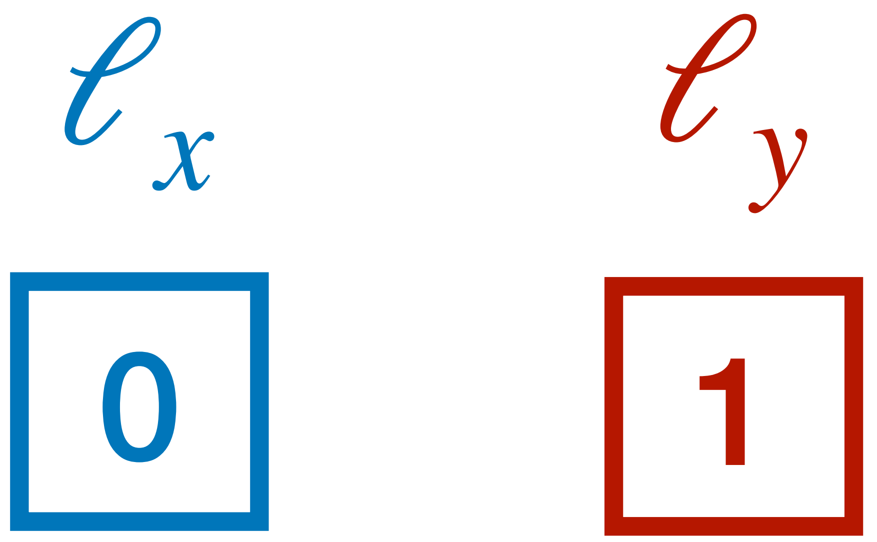
Key idea

- Probability spaces are the heaps of probability theory.

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



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



Key idea

- Probability spaces are the heaps of probability theory.

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

ℓ_x: $\boxed{0}$

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

ℓ_x: $\boxed{0}$ $\uplus$ ℓ_y: $\boxed{1}$

Key idea

- Probability spaces are the heaps of probability theory.

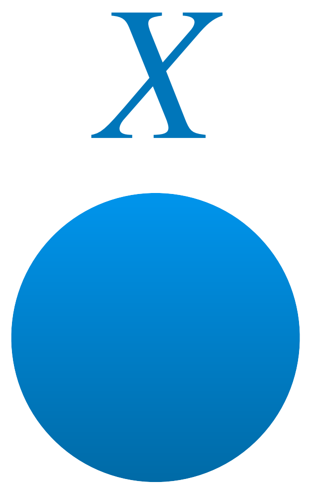
$X \leftarrow \texttt{flip}\ 1/2;$

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

Key idea

- Probability spaces are the heaps of probability theory.

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



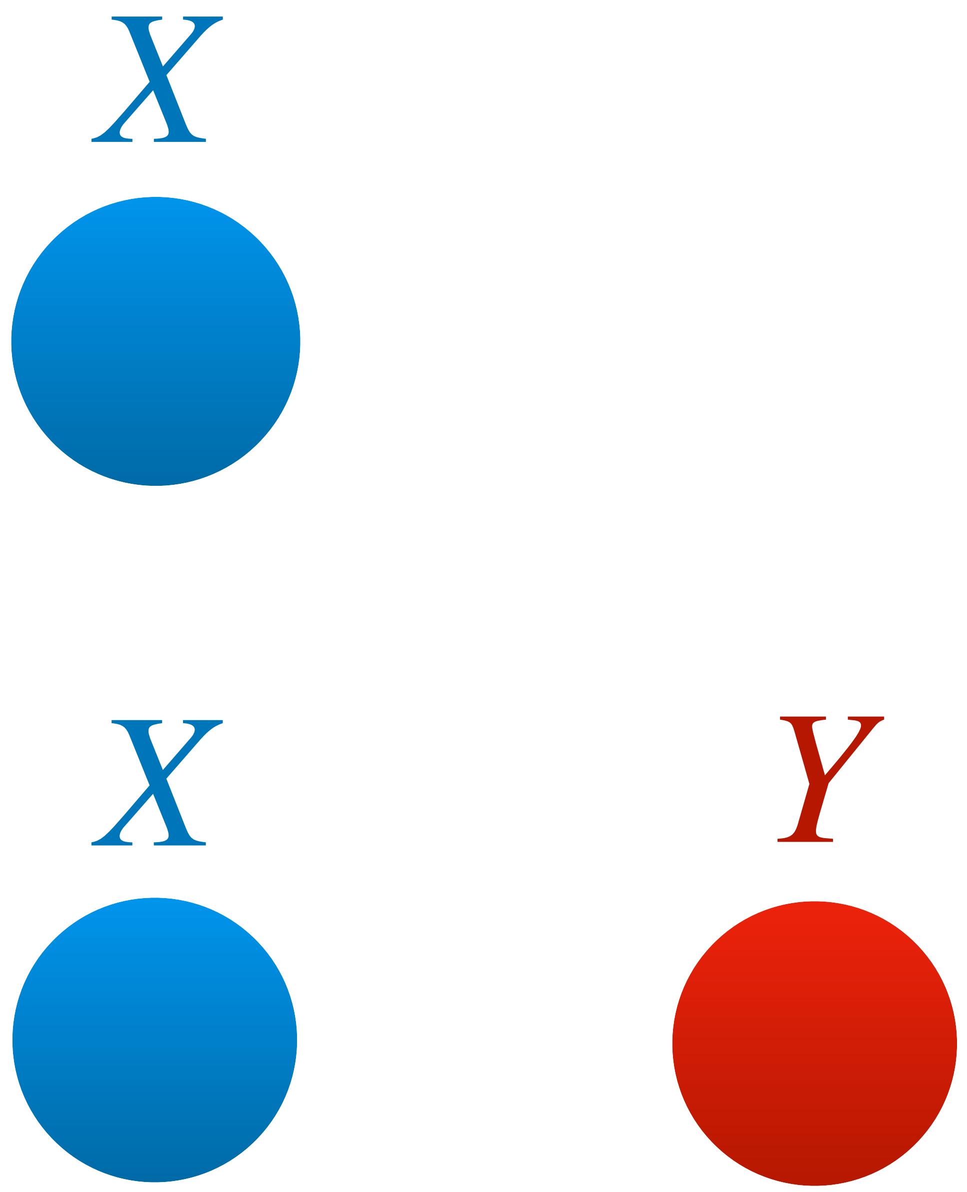
$Y \leftarrow \texttt{flip}\ 1/2;$

Key idea

- Probability spaces are the heaps of probability theory.

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

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

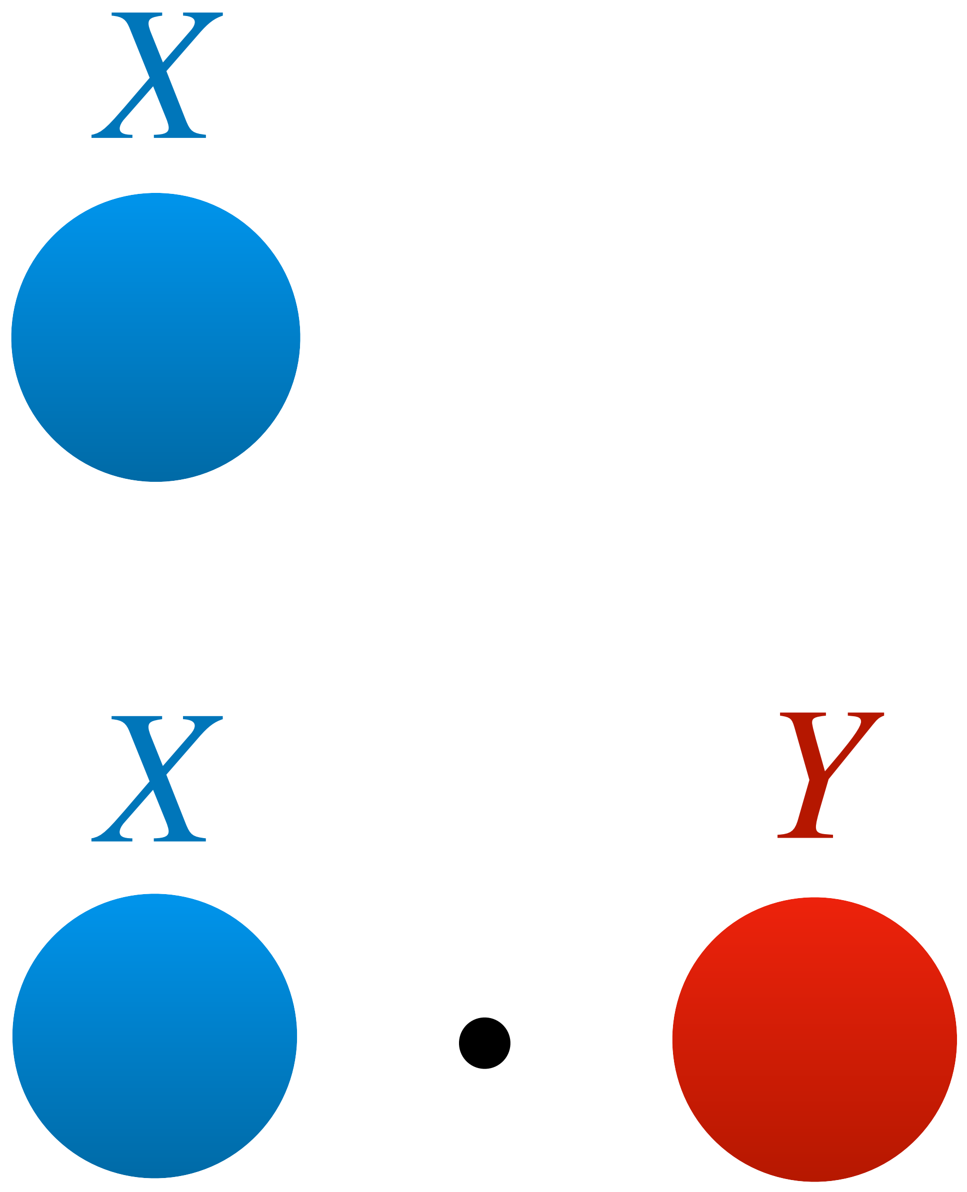


Key idea

- Probability spaces are the heaps of probability theory.

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

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

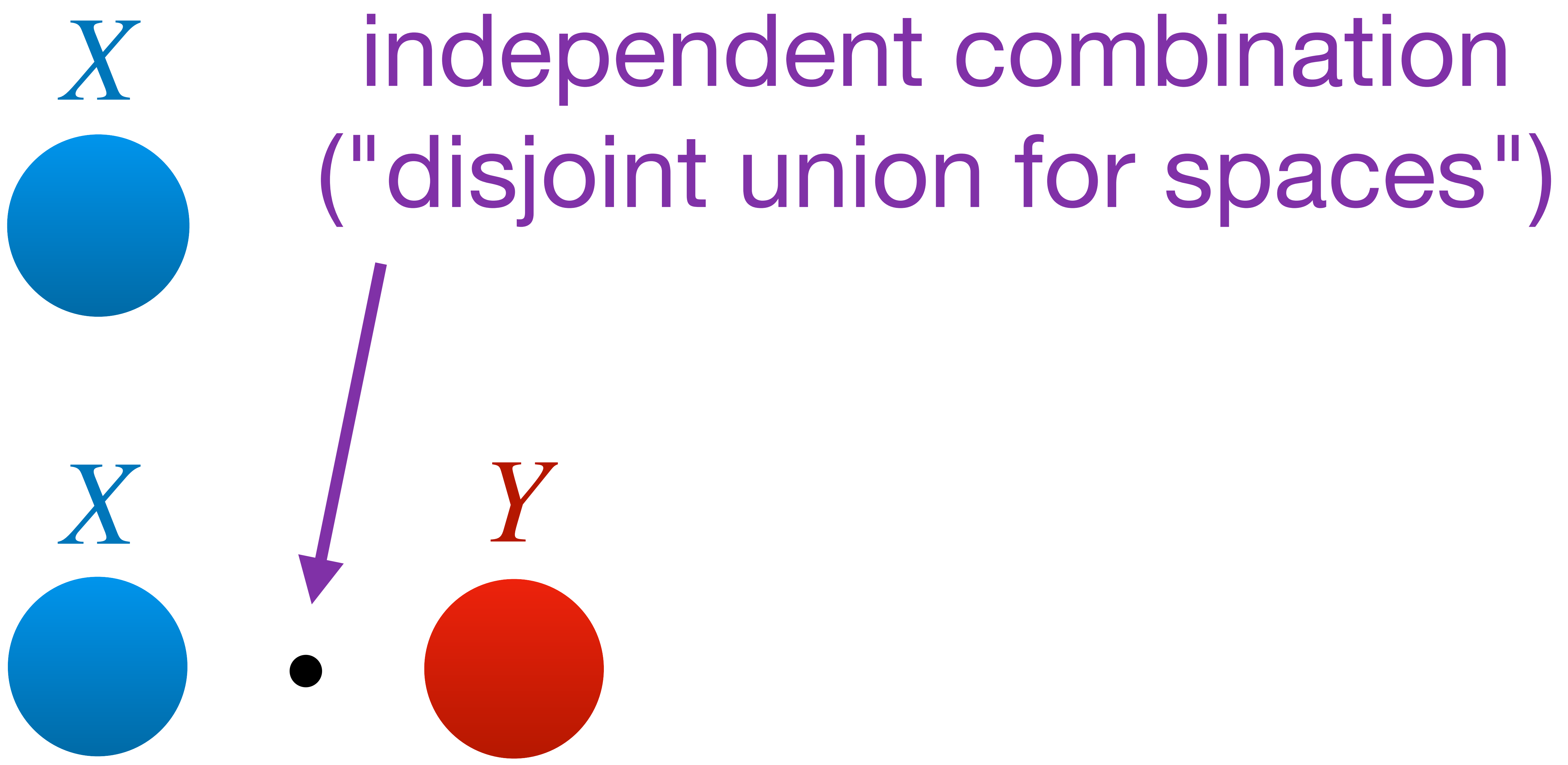


Key idea

- Probability spaces are the heaps of probability theory.

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

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

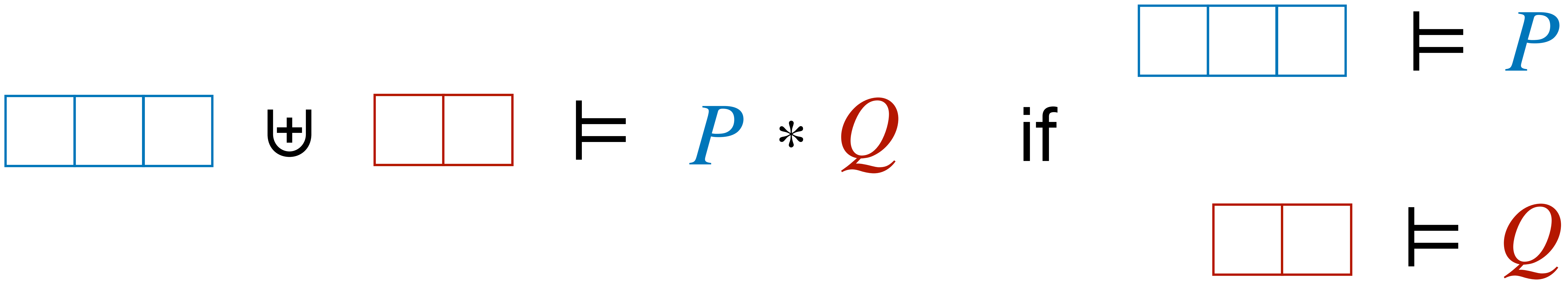


Key idea

- Probability spaces are the heaps of probability theory.
- Separating conjunction decomposes probability spaces:

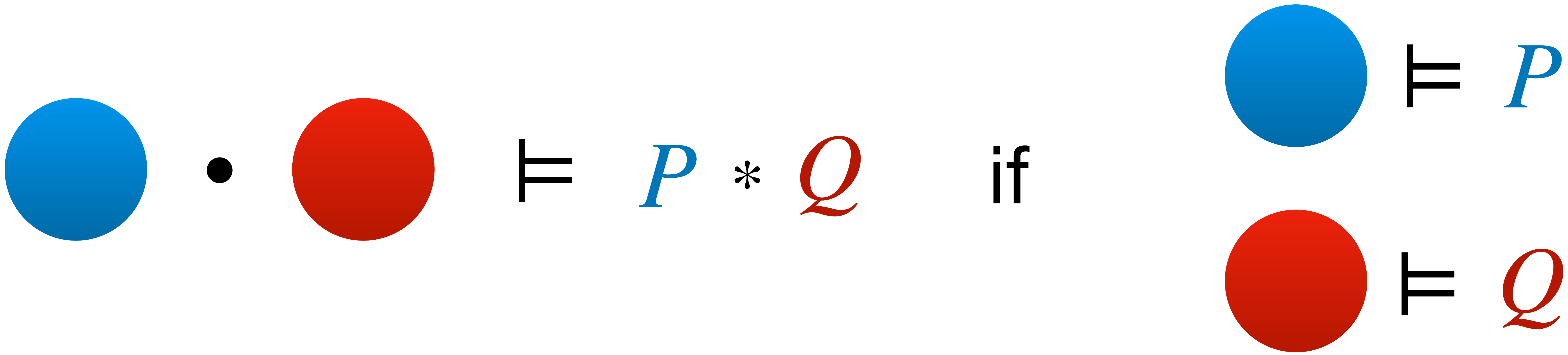
Key idea

- <u>Probability spaces are the heaps of probability theory.</u>
- Separating conjunction decomposes probability spaces:



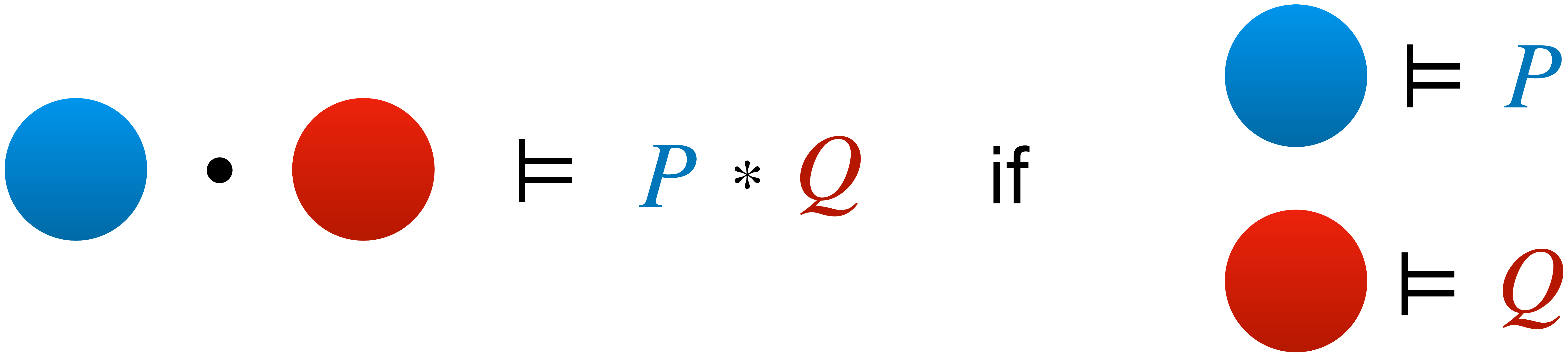
Key idea

- Probability spaces are the heaps of probability theory.
- Separating conjunction decomposes probability spaces:



Key idea

- Probability spaces are the heaps of probability theory.
- Separating conjunction decomposes probability spaces:



- $\Longrightarrow$ frame rule, star as independence, good interop, ...

Lilac: a modal separation logic for conditional probability

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*:

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*:

$$\underset{x \leftarrow X}{\mathbf{C}} \; P$$

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*:

$$\underset{x \leftarrow X}{\mathbf{C}} \; P$$

P holds conditional on $X = x$ for all x

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*:

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

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*:

X and Y are independent

↓

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

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*:

X and Y are independent

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

X and Y have distribution $\mathrm{Ber}(1/2)$

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*:

$$\underset{z \leftarrow Z}{\mathbf{C}} \left(X \sim \mathrm{Ber}(1/2) \quad * \quad Y \sim \mathrm{Ber}(1/2) \right)$$

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*:

X and Y are conditionally independent given Z

↓

$$\underset{z \leftarrow Z}{\mathbf{C}} \left(X \sim \mathrm{Ber}(1/2) \;*\; Y \sim \mathrm{Ber}(1/2) \right)$$

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*:

X and Y are conditionally independent given Z

$$\mathbf{C}_{z \leftarrow Z}\left(X \sim \mathrm{Ber}(1/2) \quad * \quad Y \sim \mathrm{Ber}(1/2) \right)$$

X and Y have conditional distribution $\mathrm{Ber}(1/2)$ given Z

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*:

$$\Pr[E] = 1/2 \qquad E \text{ has probability } 1/2$$

$$\mathbf{E}[X] = 0 \qquad X \text{ has expectation } 0$$

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*:

$$\underset{x \leftarrow X}{\mathbf{C}}\left(\Pr[E] = 1/2\right) \qquad E \text{ has probability } 1/2 \text{ given } X = x$$

$$\mathbf{E}[X] = 0 \qquad X \text{ has expectation } 0$$

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*:

$$\underset{x \leftarrow X}{\mathbf{C}} \left(\Pr[E] = 1/2 \right)$$

E has probability $1/2$ given $X = x$

$$\underset{y \leftarrow Y}{\mathbf{C}} \left(\mathbf{E}[X] = 0 \right)$$

X has conditional expectation 0

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*
- Laws express intuitive facts and standard theorems:

Lilac: a modal separation logic for conditional probability

- Conditioning as a *modality*
- Laws express intuitive facts and standard theorems:

C-Total-Expectation

$$\underset{x \leftarrow X}{\mathbf{C}} \left(\mathbb{E}[E] = e \right) \;\land\; \mathbb{E}[e[X/x]] = v \vdash \mathbb{E}[E] = v$$

We used Lilac to verify

- Examples from prior work (cryptographic protocols)
- A tricky weighted sampling algorithm exercising
  - Continuous random variables
  - Quantitative reasoning
  - Separation as independence
  - Conditioning modality

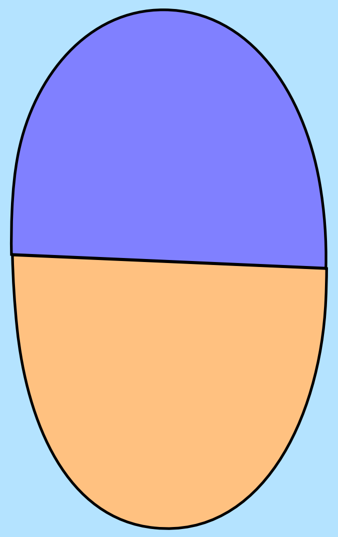
Also in the paper

- Conditioning modality
- Ownership is measurability
- Worked examples
- Almost-sure equality $X =_{\text{a.s.}} Y$

Thanks!

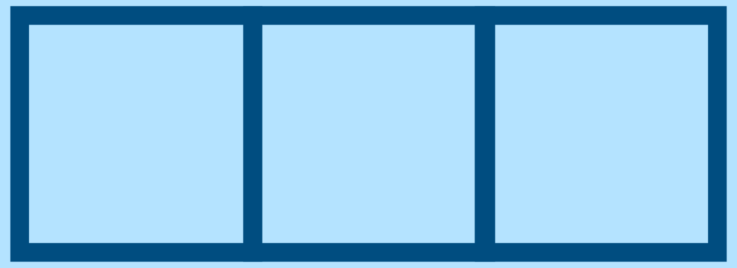
Probability theory $\simeq$ Mutable references

X



$(\Omega, \text{events}, \mu)$

ℓ



h

https://johnm.li/lilac.pdf

li.john@northeastern.edu