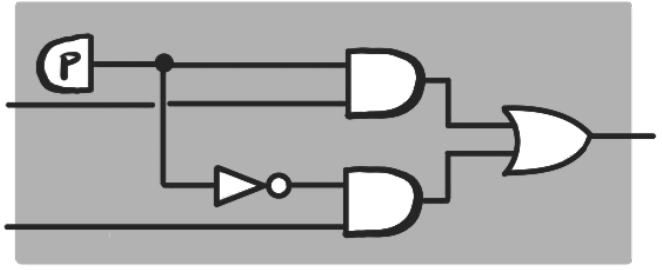
THE ALGEBRA OF PROBABILISTIC BOOLEAN CIRCUITS

Robin Piedeleu
UCL Computer Science



Tallinn Workshop on Computing with Markov Categories
26 Feb. 2025

Mateo Torres-Ruiz
UCL

Alexandra Silva
Cornell University

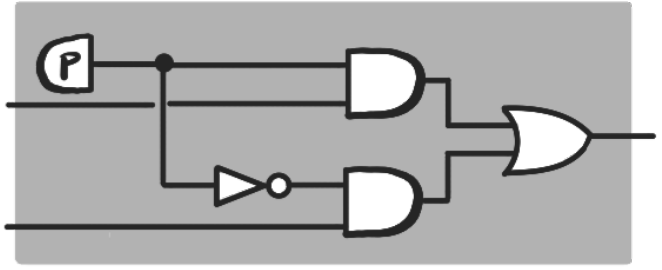
Fabio Zanasi
UCL

A Complete Axiomatisation of Equivalence for Discrete Probabilistic Programs, ESOP '25

arXiv: 2408.14701

THE ALGEBRA OF PROBABILISTIC BOOLEAN CIRCUITS

Robin Piedeleu
UCL Computer Science

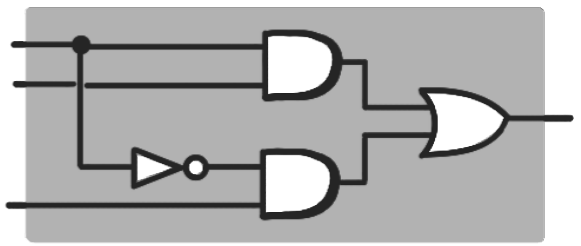


Tallinn Workshop on Computing with Markov Categories
26 Feb. 2025

QUESTION

syntax ? semantics ?
equational theory ?

Boolean circuits + Randomness = ?



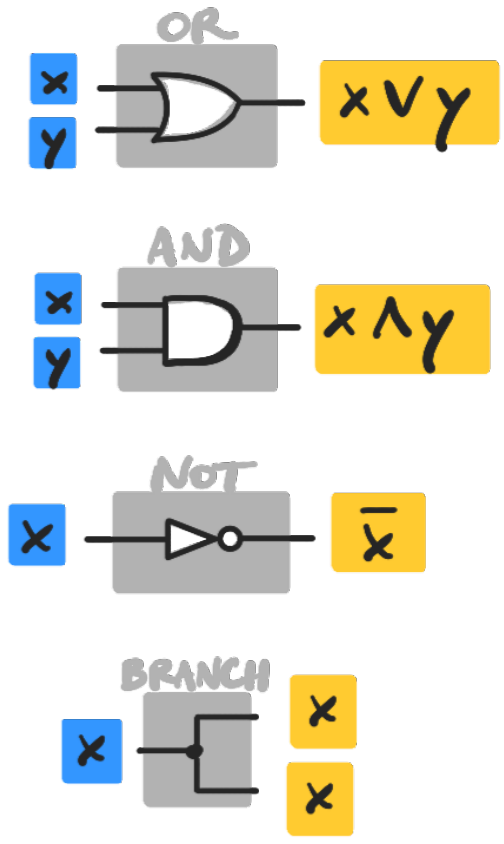
OUTLINE

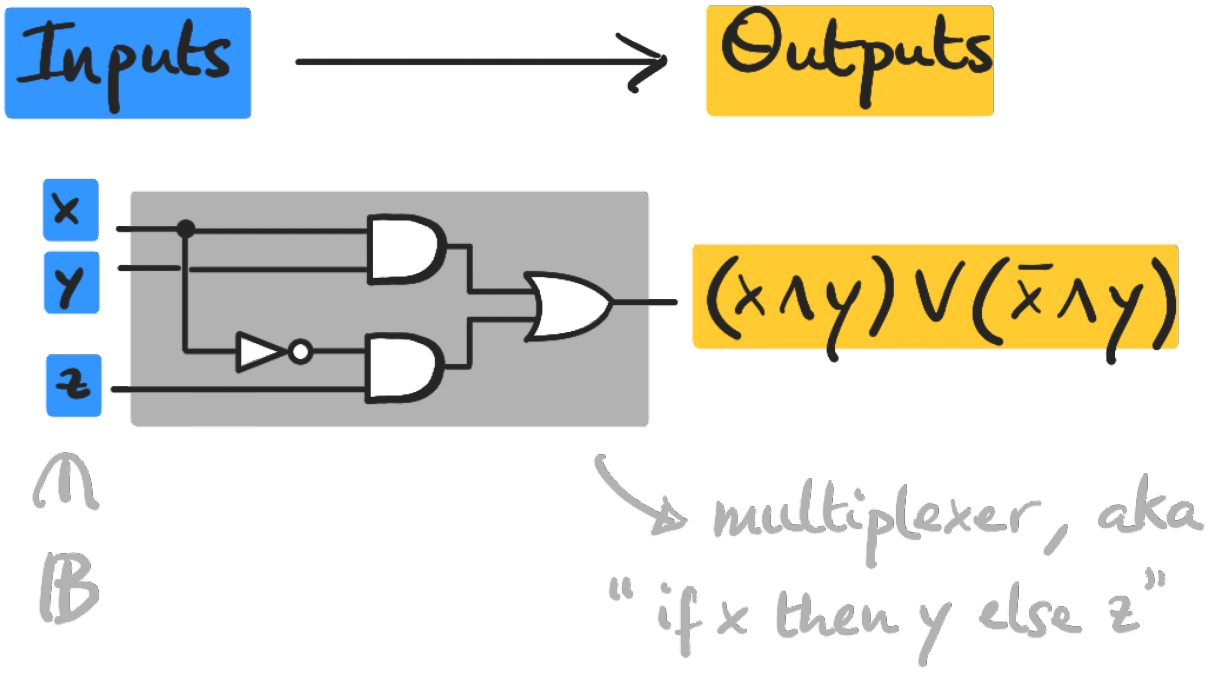
1. BOOLEAN CIRCUITS (PROP-Style)
2. PROBABILISTIC BOOLEAN CIRCUITS
3. PROBABILISTIC (BOOLEAN) PROGRAMMING
4. CONCLUSION

OUTLINE

1. BOOLEAN CIRCUITS (PROP-Style)
2. PROBABILISTIC BOOLEAN CIRCUITS
3. PROBABILISTIC (BOOLEAN) PROGRAMMING
4. CONCLUSION

BOOLEAN CIRCUITS



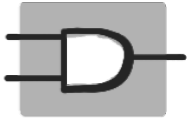


BOOLEAN CIRCUITS

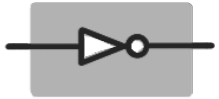
Functorial semantics

Symmetric monoidal functor

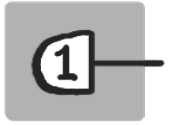
$$\underline{\mathbf{BoolCirc}} \simeq \text{Free PROP generated by (e.g.)} \xrightarrow{[\![-]\!]} (\underline{\mathbf{Set}}_{\mathbb{B}}, \times, 1)$$



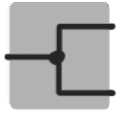
$$[\![-]\!] : \mathbb{B}^2 \ni (x, y) \mapsto x \wedge y$$



$$[\![-]\!] : \mathbb{B} \ni x \mapsto \bar{x}$$



$$[\![-]\!] : \mathbb{B}^0 \ni \bullet \mapsto 1 \ (\text{true})$$



$$[\![-]\!] : \mathbb{B} \ni x \mapsto (x, x)$$

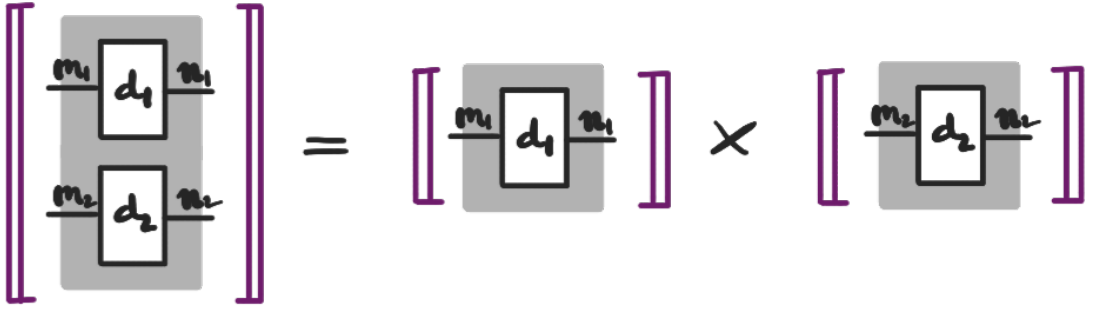
$$[\![-]\!] : \mathbb{B} \ni x \mapsto \bullet$$

BOOLEAN CIRCUITS

Functorial semantics

Symmetric monoidal functor

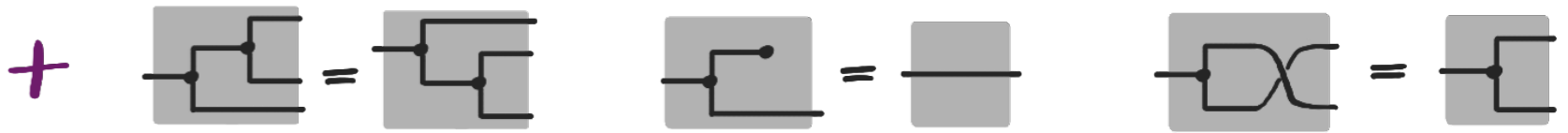
$$\mathbf{BoolCirc} \xrightarrow{[\![-]\!]} (\mathbf{Set}_{\mathbb{B}}, \times, 1)$$



BOOLEAN CIRCUITS

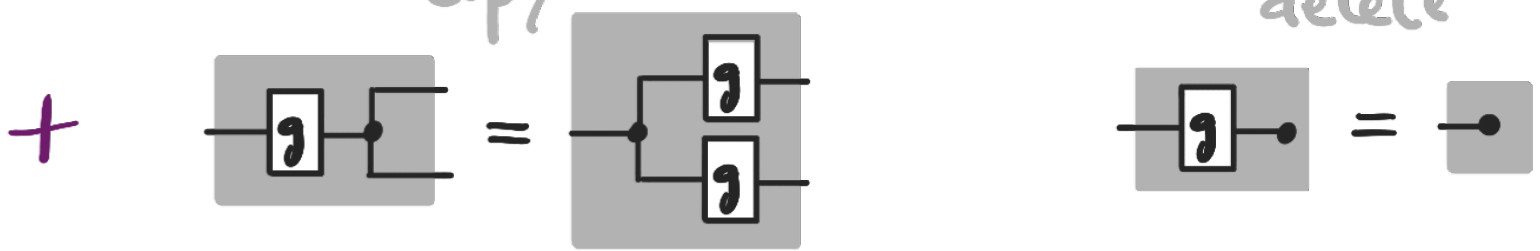
Equational theory

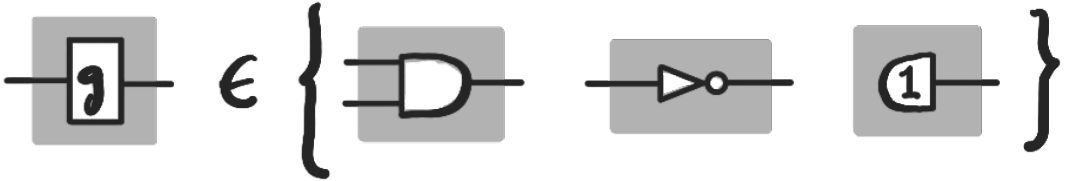
Axioms of Boolean algebra [Boole, 1850s]



Copy

delete



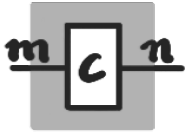
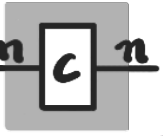
for 

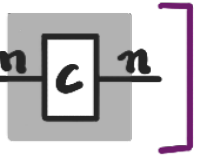
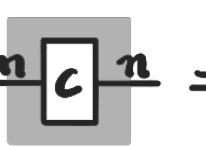
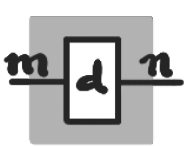
BOOLEAN CIRCUITS

Complete presentation

Theorem. [Lafont, 2003?] The PROP **BoolCirc** quotiented by the axioms of Boolean algebra + Copy-Delete is isomorphic to the PROP of Boolean functions

SMF $[-]$

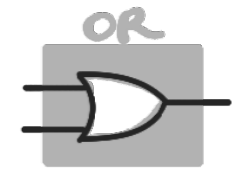
① **Full**: for every $f : \mathbb{B}^m \to \mathbb{B}^n$, there exists  s.t. $\left[\right.$  $\left.\right] = f$

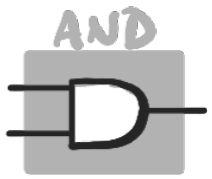
② **Faithful**: $\left[\right.$  $\left.\right] = \left[\right.$  $\left.\right] \Rightarrow$  $=$ 

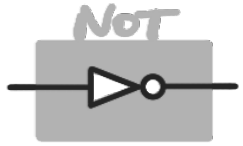
OUTLINE

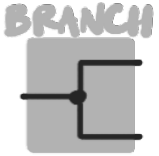
1. BOOLEAN CIRCUITS (PROP-style)
2. PROBABILISTIC BOOLEAN CIRCUITS
3. PROBABILISTIC (BOOLEAN) PROGRAMMING
4. CONCLUSION

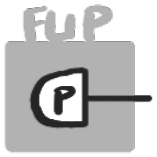
Probabilistic Boolean Circuits



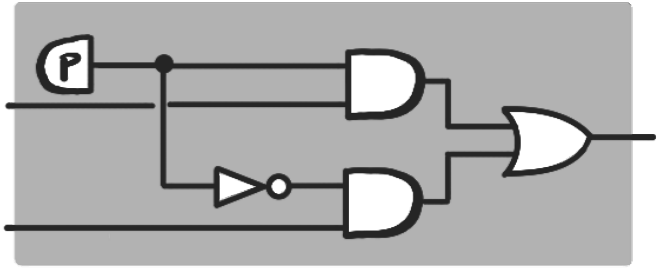








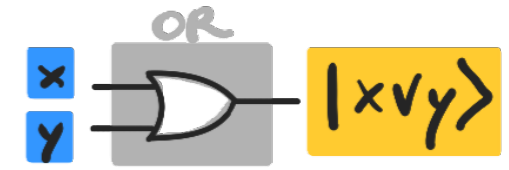
Inputs → ?

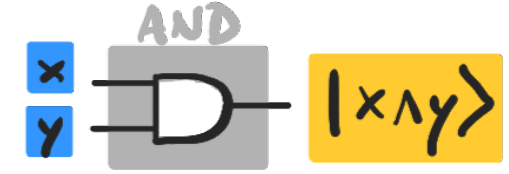


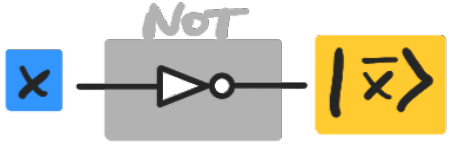
1 with probability $p \in [0,1]$

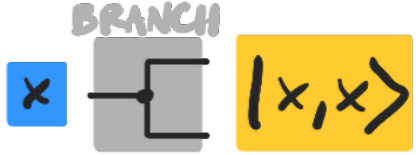
0 with probability $1-p$

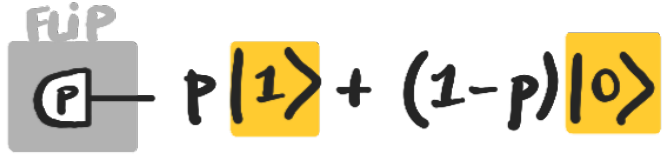
PROBABILISTIC BOOLEAN CIRCUITS





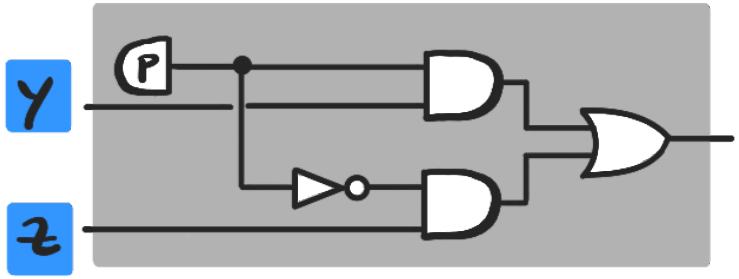






distributions

Inputs ⟶ $\mathcal{D}$(Outputs)



"p-convex sum of y & z"

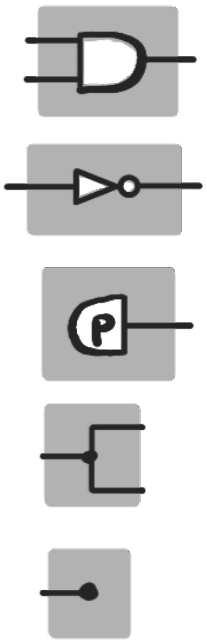
N.B. $|\vec{x}\rangle$ is the Dirac distribution at $\vec{x} \in \mathbb{B}^n$

Probabilistic Boolean Circuits

Stochastic maps

$$\mathbf{ProbCirc} \xrightarrow{[\![-]\!]} (\mathbf{Stoch}_{\mathbb{B}}, \times, 1)$$

$\mathbf{ProbCirc}$ = Free PROP generated by



$$[\![-]\!]: \mathbb{B}^2 \ni (x,y) \mapsto |x \wedge y\rangle$$

$$[\![-]\!]: \mathbb{B} \ni x \mapsto |\bar{x}\rangle$$

$$[\![-]\!]: \mathbb{B}^0 \ni \bullet \mapsto (1-p)|0\rangle + p|1\rangle$$

$$[\![-]\!]: \mathbb{B} \ni x \mapsto |x,x\rangle$$

$$[\![-]\!]: \mathbb{B} \ni x \mapsto |\bullet\rangle$$

only distribution on one element

Probabilistic Boolean circuits

Stochastic maps

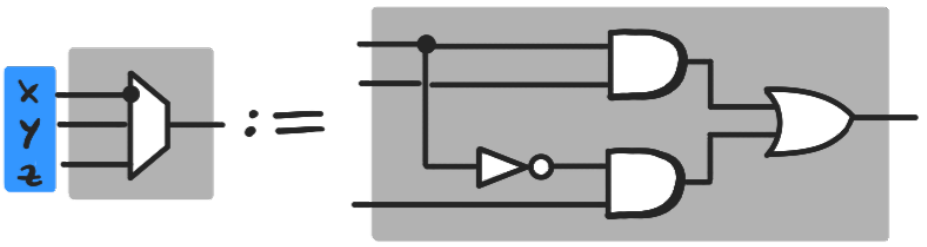
$$\mathbf{ProbCirc} \xrightarrow[\text{Symmetric monoidal functor}]{[\![-]\!]} (\mathbf{Stoch}_{\mathbb{B}}, \times, 1)$$

$$\left[\!\!\left[\begin{array}{c} \ell \\ \boxed{c} \\ m \end{array} \;\; \begin{array}{c} m \\ \boxed{d} \\ n \end{array} \right]\!\!\right](z|x) = \sum_{y \in \mathbb{B}^m} \left[\!\!\left[\begin{array}{c} m \\ \boxed{d} \\ n \end{array} \right]\!\!\right](z|y) \cdot \left[\!\!\left[\begin{array}{c} \ell \\ \boxed{c} \\ m \end{array} \right]\!\!\right](y|x)$$

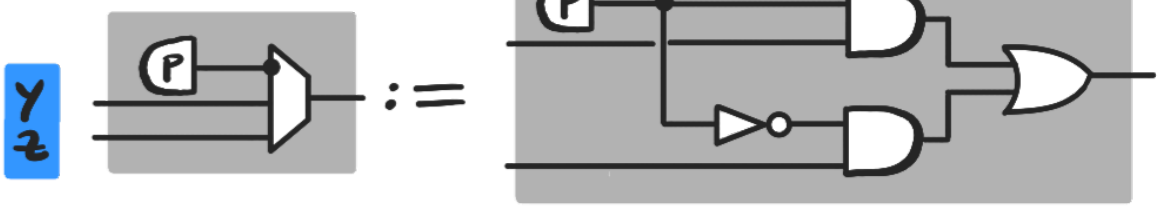
$$\left[\!\!\left[\begin{array}{c} m_1 \\ \boxed{d_1} \\ n_1 \end{array} \;\; \begin{array}{c} m_2 \\ \boxed{d_2} \\ n_2 \end{array} \right]\!\!\right](y_1, y_2 | x_1, x_2) = \left[\!\!\left[\begin{array}{c} m_1 \\ \boxed{d_1} \\ n_1 \end{array} \right]\!\!\right](y_1|x_1) \cdot \left[\!\!\left[\begin{array}{c} m_2 \\ \boxed{d_2} \\ n_2 \end{array} \right]\!\!\right](y_2|x_2)$$

NOTATION

We can define **if-then-else** as syntactic sugar:



$$\begin{cases} |y\rangle & \text{if } x = 1 \\ |z\rangle & \text{if } x = 0 \end{cases}$$



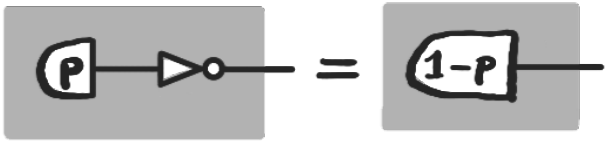
$$p|y\rangle + (1-p)|z\rangle$$

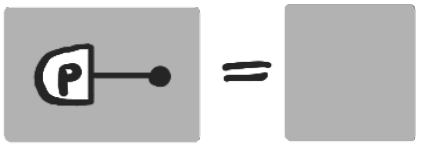
"p-convex sum of y & z"

PROBABILISTIC BOOLEAN CIRCUITS

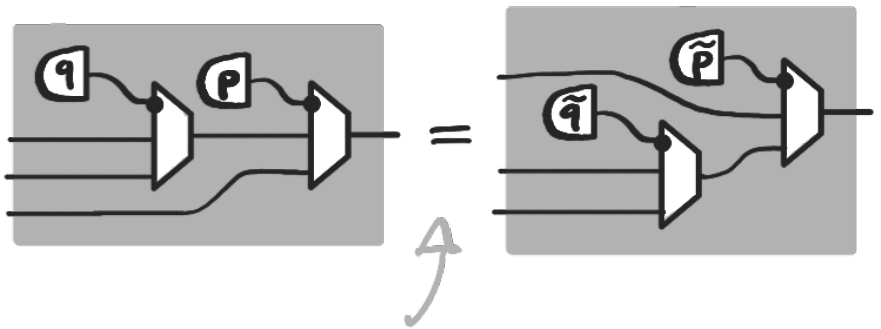
Equational theory (1/3)

Axioms of Boolean circuits +





Bernoulli(p) is a normalised probability dist.



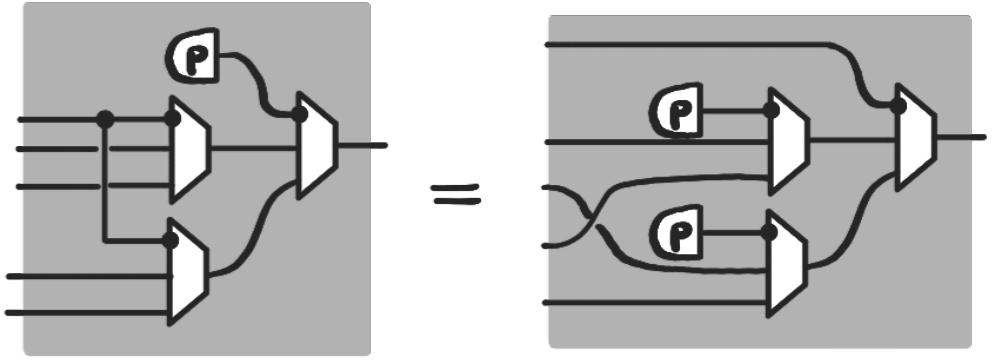
where $\begin{cases} \tilde{p} = pq \\ \tilde{q} = \dfrac{p(1-q)}{1-pq} \end{cases}$ for $pq \neq 1$

M. Stone, Postulates for the barycentric calculus, 1949

T. Fritz, A presentation of the category of stochastic matrices, 2009

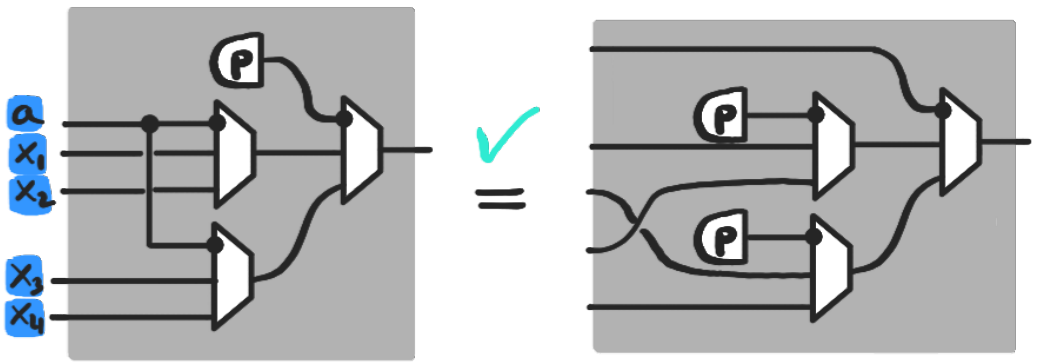
Probabilistic Boolean Circuits

Equational theory (2/3)



Probabilistic Boolean Circuits

Equational theory (2/3)



$$\begin{cases} p|x_1\rangle + (1-p)|x_3\rangle & \text{if } a=1 \\ p|x_2\rangle + (1-p)|x_4\rangle & \text{if } a=0 \end{cases}$$

Probabilistic Boolean Circuits

Equational theory (3/3)

Two different ways to represent* a distribution over $\mathbb{B} \times \mathbb{B}$:

① ②

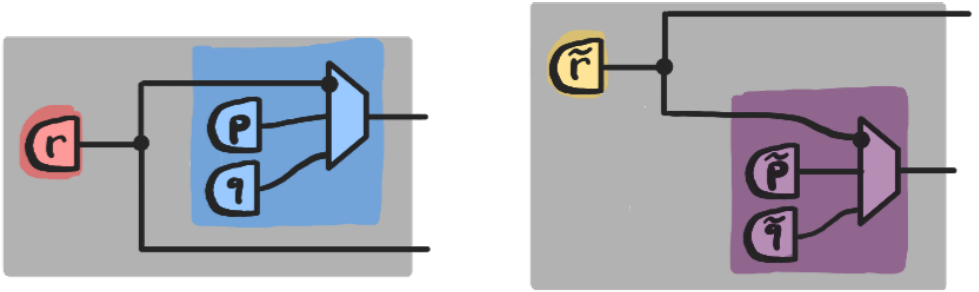
$$p(x,y) = p(x|y)\,p(y) = p(x)\,p(y|x)$$

* disintegrate

Probabilistic Boolean Circuits

Equational theory (3/3)

Two different ways to represent a distribution over $\mathbb{B} \times \mathbb{B}$:



① ②

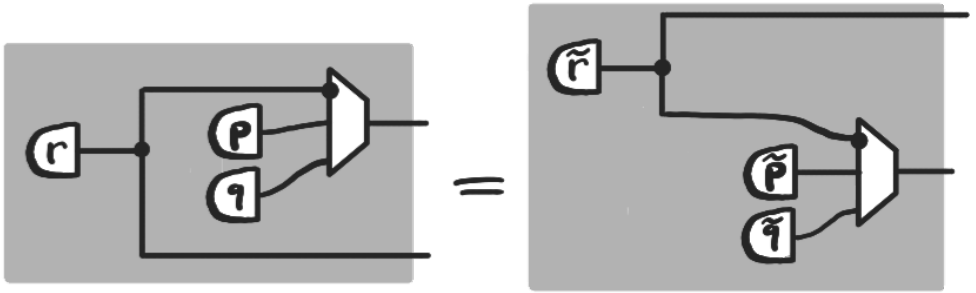
$$p(x,y) = p(x|y)\,p(y) = p(x)\,p(y|x)$$

↳ given by two Bernoullis $\begin{cases} p(x|y=0) \\ p(x|y=1) \end{cases}$

Probabilistic Boolean Circuits

Equational theory (3/3)

Two different ways to represent a distribution over $\mathbb{B} \times \mathbb{B}$:



condition on first wire

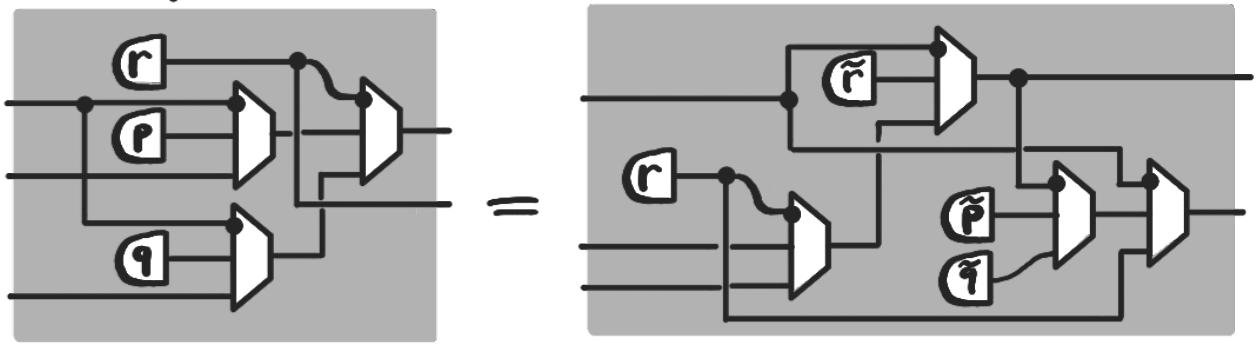
where

$$\tilde{r} = \underbrace{rp + (1-r)q}_{\text{r-convex sum of } p,q} \quad \text{and} \quad \begin{cases} \tilde{p} = \dfrac{rp}{\tilde{r}} & \text{if } \tilde{r} \neq 0 \text{ ; anything otherwise} \\ \tilde{q} = \dfrac{r(1-p)}{1-\tilde{r}} & \text{if } \tilde{r} \neq 1 \text{ ; anything otherwise} \end{cases}$$

Probabilistic Boolean Circuits

Equational theory (3/3)

Two different ways to represent a distribution over $\mathbb{B} \times \mathbb{B}$:



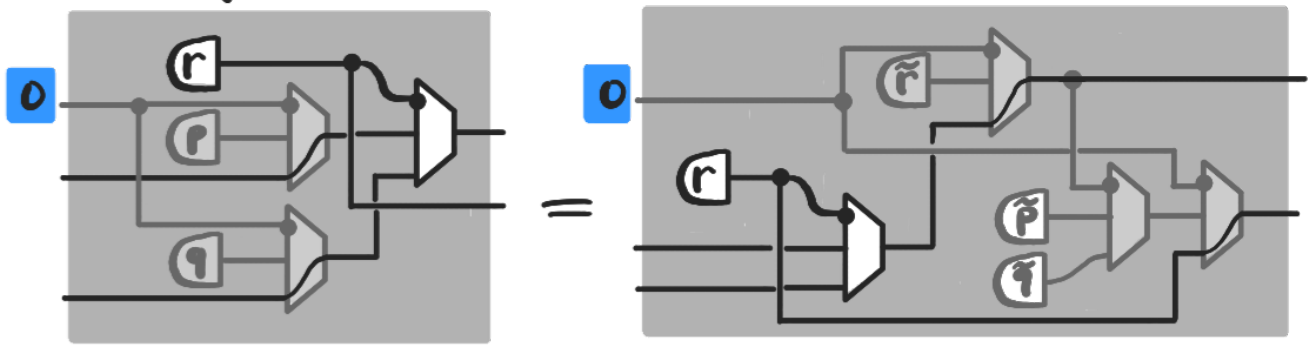
where

$$\tilde{r} = rp + (1-r)q \text{ and } \begin{cases} \tilde{p} = \dfrac{rp}{\tilde{r}} & \text{if } \tilde{r} \neq 0 \text{ ; anything otherwise} \\ \tilde{q} = \dfrac{r(1-p)}{1-\tilde{r}} & \text{if } \tilde{r} \neq 1 \text{ ; anything otherwise} \end{cases}$$

Probabilistic Boolean Circuits

Equational theory (3/3)

Two different ways to represent a distribution over $\mathbb{B} \times \mathbb{B}$:



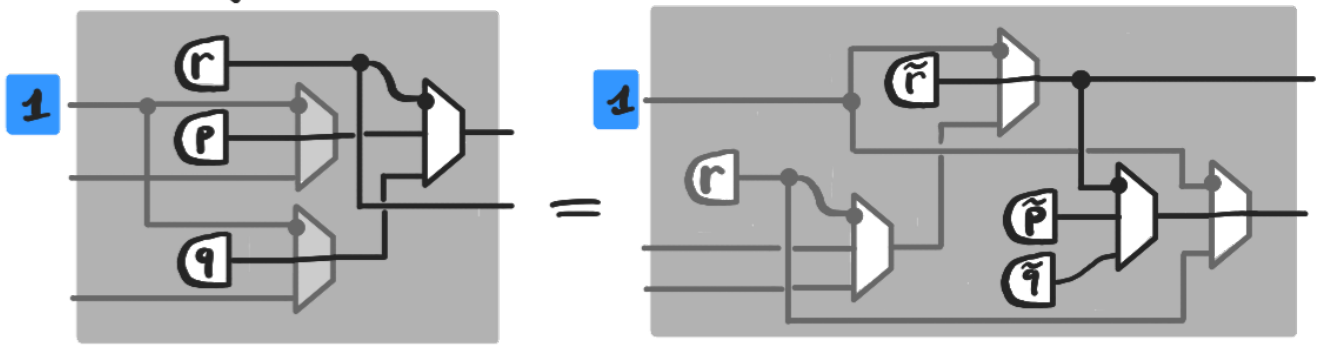
where

$$\tilde{r} = rp + (1-r)q \quad \text{and} \quad \begin{cases} \tilde{p} = \dfrac{rp}{\tilde{r}} & \text{if } \tilde{r} \neq 0 \text{ ; anything otherwise} \\ \tilde{q} = \dfrac{r(1-p)}{1-\tilde{r}} & \text{if } \tilde{r} \neq 1 \text{ ; anything otherwise} \end{cases}$$

Probabilistic Boolean Circuits

Equational theory (3/3)

Two different ways to represent a distribution over $\mathbb{B} \times \mathbb{B}$:



where

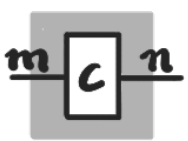
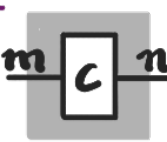
$$\tilde{r} = rp + (1-r)q \quad \text{and} \quad \begin{cases} \tilde{p} = \dfrac{rp}{\tilde{r}} & \text{if } \tilde{r} \neq 0 \text{ ; anything otherwise} \\ \tilde{q} = \dfrac{r(1-p)}{1-\tilde{r}} & \text{if } \tilde{r} \neq 1 \text{ ; anything otherwise} \end{cases}$$

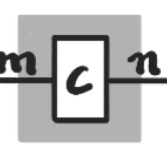
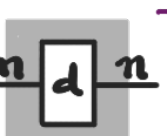
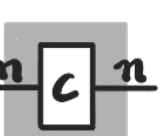
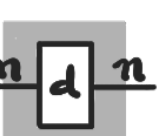
PROBABILISTIC BOOLEAN CIRCUITS

Complete presentation

Theorem. The PROP **ProbCirc** quotiented by the axioms above is isomorphic to the PROP of stochastic maps of type $\mathbb{B}^m \to\!\!\!\!\to \mathbb{B}^n$.

$[-]$

① **Full**: for every stochastic map $f : \mathbb{B}^m \to\!\!\!\!\to \mathbb{B}^n$, there exists  s.t. $\left[\right.$  $\left.\right] = f$

② **Faithful**: $\left[\right.$  $\left.\right] = \left[\right.$  $\left.\right] \Rightarrow$  $=$ 

OUTLINE

1. BOOLEAN CIRCUITS (PROP-style)
2. PROBABILISTIC BOOLEAN CIRCUITS
3. PROBABILISTIC (BOOLEAN) PROGRAMMING
4. CONCLUSION

Probabilistic (Boolean) Programming

An example

```
first = flip p;
second = flip p;
observe (first = ! second);
return first
```

Von Neumann's trick to simulate a fair coin with a biased one:

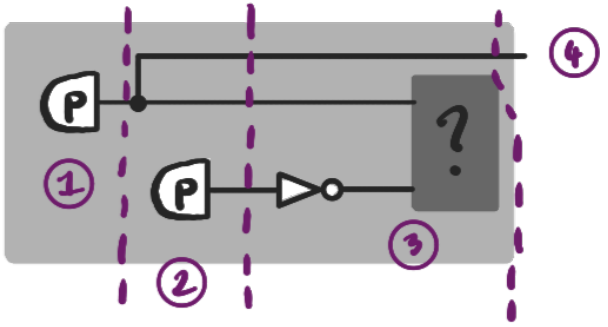
× 2;

if the outcomes are the same, discard and start over;
if the outcomes are different, keep (e.g.) the first.

Probabilistic (Boolean) Programming

An example

VonNeumann's trick

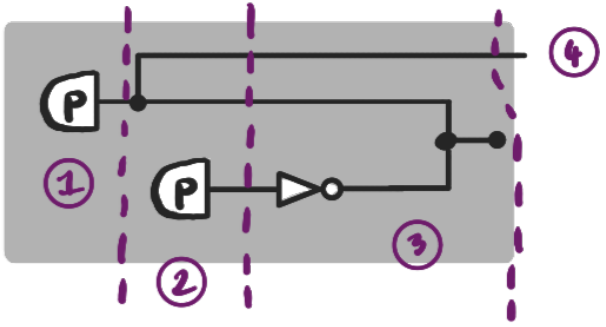



```
① first = flip p;
② second = flip p;
③ observe (first =! second);
④ return first
```

PROBABILISTIC (BOOLEAN) PROGRAMMING

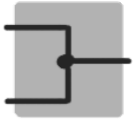
An example

VonNeumann's trick




```
① first = flip p ;
② second = flip p ;
③ observe (first =! second);
④ return first
```

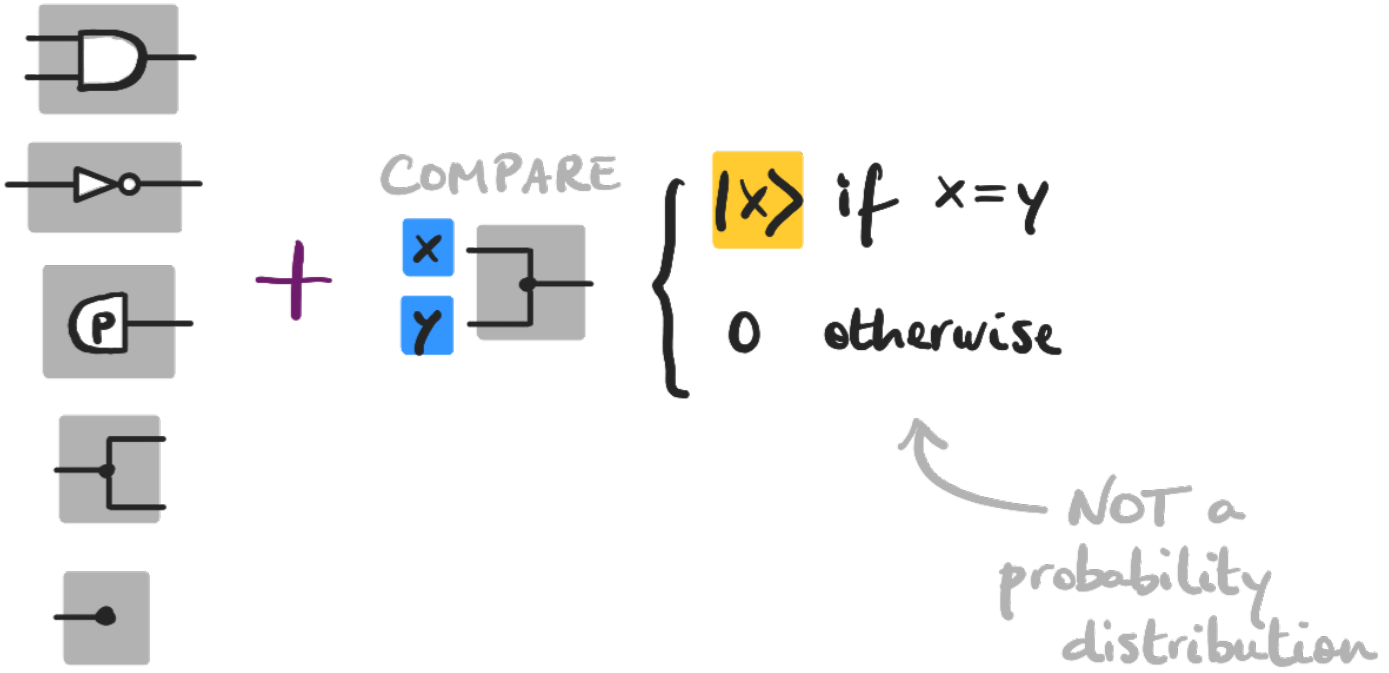
where



imposes the condition that its two inputs are equal

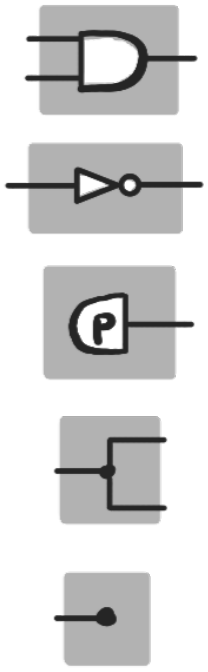
Probabilistic (Boolean) Programming

Adding first-class conditioning



Probabilistic (Boolean) Programming

Adding first-class conditioning



sub distributions

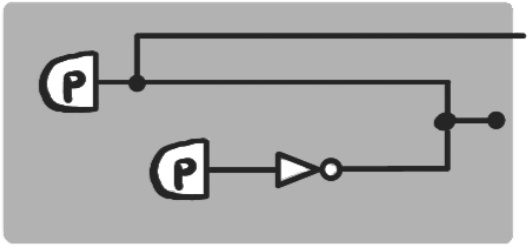
Inputs → $\mathcal{D}_{\leq 1}$(Outputs)

$$\begin{cases} |x\rangle & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$

Probabilistic (Boolean) Programming

An example, semantically

Von Neumann's trick



$$\xrightarrow{[\![-]\!]} \quad p(1-p)\,|1\rangle + (1-p)\,p\,|0\rangle$$

$$\neq$$

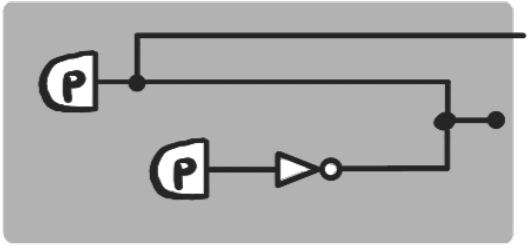
$$\frac{1}{2}|1\rangle + \frac{1}{2}|0\rangle$$

in general

Probabilistic (Boolean) Programming

An example, semantically

VonNeumann's trick



$$\xrightarrow{[\![-]\!]} \quad p(1-p)\,|1\rangle + (1-p)\,p\,|0\rangle$$

$$\propto$$

$$\tfrac{1}{2}|1\rangle + \tfrac{1}{2}|0\rangle$$

"proportional"

Probabilistic (Boolean) Programming

Semantics

Definition. For $f, g : X \longrightarrow \mathcal{D}_{\leq 1}(Y)$ we write $f \propto g$ if there exists a real number $\lambda > 0$ s.t. $f(x) = \lambda \cdot g(x)$ for all $x \in X$.

Proposition [Stein & Staton, 2023] Substochastic maps up to $\propto$ form a symmetric monoidal category (with the $\times$)

$$[\![-]\!] : \text{ProbCirc} + \quad \longrightarrow \quad (\underline{\text{Proj}}\underline{\text{Stoch}}, \times, 1)$$

$$\quad \longmapsto \quad \Big[(x,y) \mapsto \begin{cases} |x\rangle \text{ if } x = y \\ 0 \quad \text{otherwise} \end{cases} \Big]_{\propto}$$

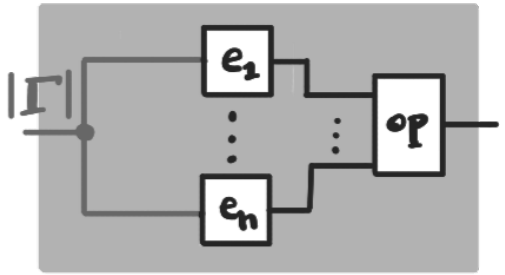
equivalence class

Probabilistic (Boolean) Programming

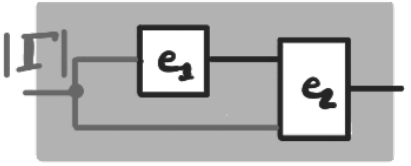
Code as diagrams, diagrams as code

Context = list of free variables

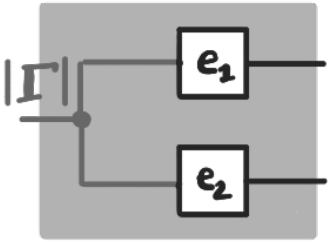
$\Gamma \vdash op(e_1, \ldots, e_n)$



$\Gamma \vdash \text{let } x = e_1 \text{ in } e_2$

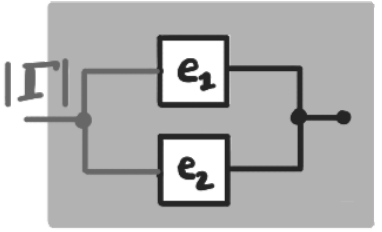


$\Gamma \vdash \langle e_1, e_2 \rangle$



$\Gamma \vdash \text{flip } p$

$\Gamma \vdash \text{observe}(e_1 == e_2)$

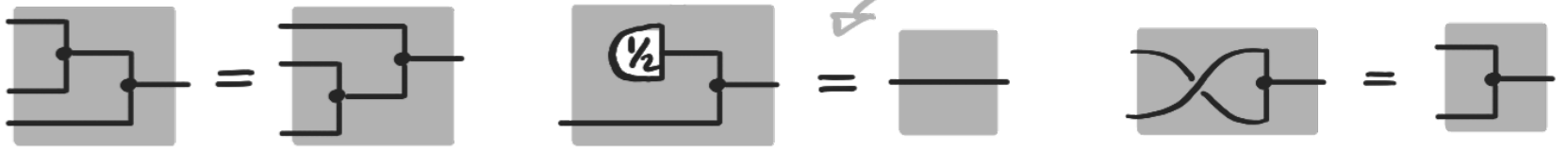


Probabilistic (Boolean) Programming

Equational theory (1/2)

Axioms of probabilistic circuits +

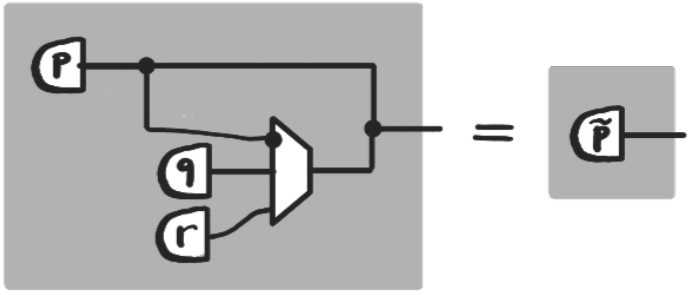
only valid up to $\propto$



(special Frobenius algebra)

Probabilistic (Boolean) Programming

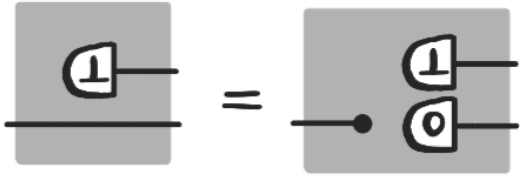
Equational theory (2/2)



$=$

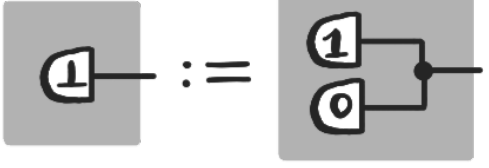
$$\tilde{p} := \frac{pq}{pq + (1-p)(1-r)}$$

↳ if non zero



$=$

where

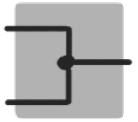


$:=$

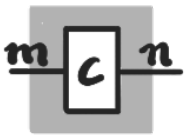
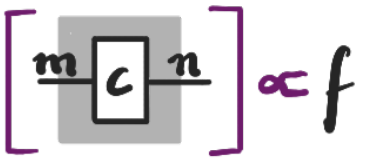
failure, aka the zero subdistribution

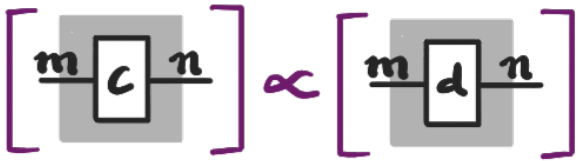
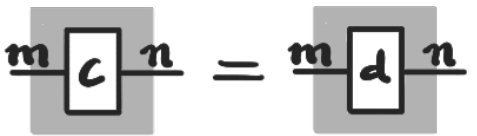
PROBABILISTIC (BOOLEAN) PROGRAMMING

Complete presentation

Theorem. The PROP ProbCirc +  quotiented by the axioms above is isomorphic to the PROP of substochastic maps of type $\mathbb{B}^m \to \mathbb{B}^n$, modulo $\propto$.

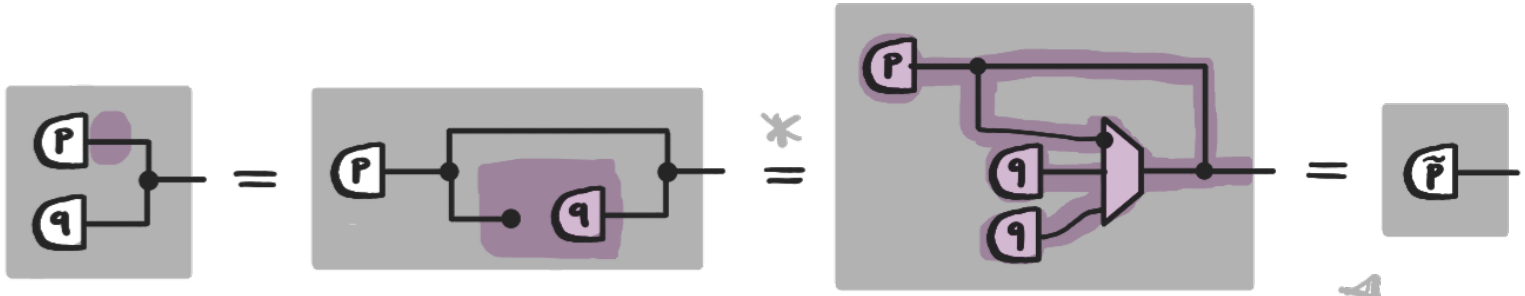
$[-]$

① **Full**: for every substochastic map $f : \mathbb{B}^m \to \mathbb{B}^n$, there exists  s.t.  $\propto f$

② **Faithful**:  $\Rightarrow$ 

VERIFYING VON NEUMANN'S TRICK

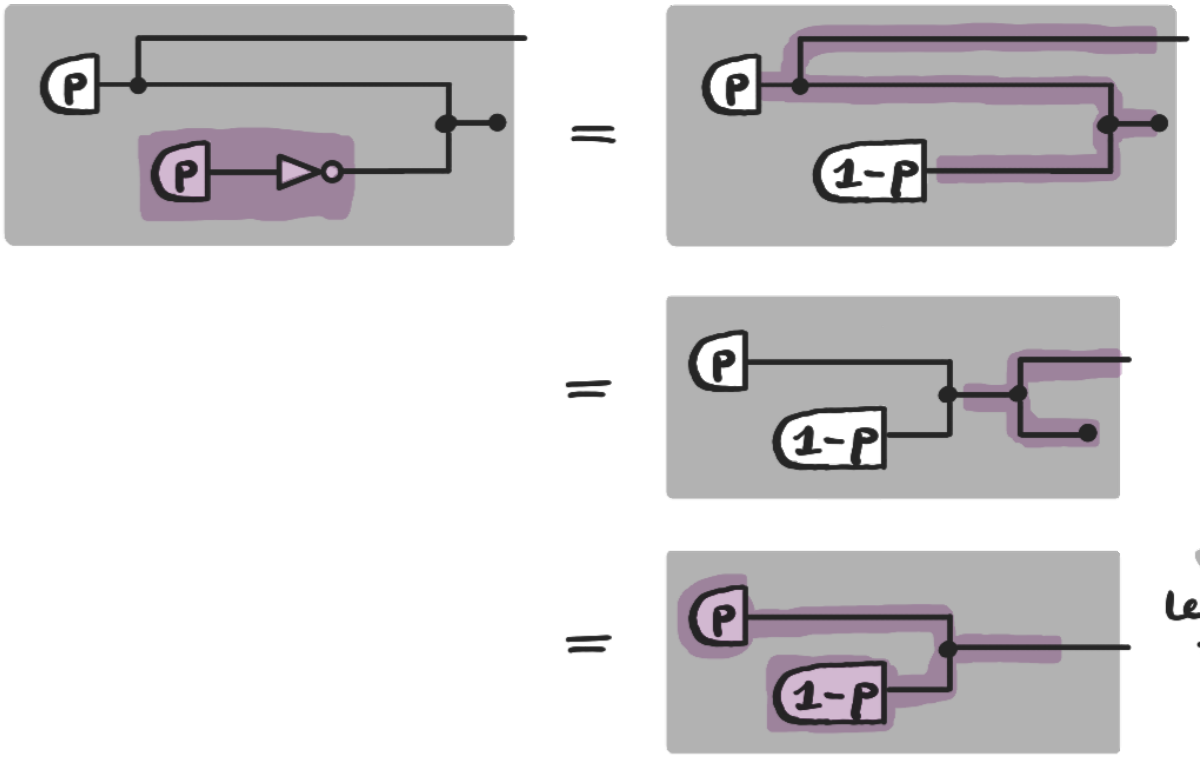
Lemma. For $p, q \in (0,1)$



with $$\tilde{p} := \frac{pq}{pq + (1-p)(1-q)}$$

* trust me

VERIFYING VON NEUMANN'S TRICK



$$\frac{p(1-p)}{p(1-p)+(1-p)p} = \frac{1}{2}$$

Discussion

- Can we extend the axiomatisation to substochastic maps (not modulo $\propto$) ?
- Quantitative reasoning with KL-divergence, total variation ... ? [Perrone, 2023]
- Combine with work on Gaussian programming [Stein et al, 24] for mixtures of Gaussians (talk to Mateo about it !)

Stein, Zanasi, P., Samuelson, Graphical Quadratic Algebra, 2024
Perrone, Markov Categories & Entropy, 2023