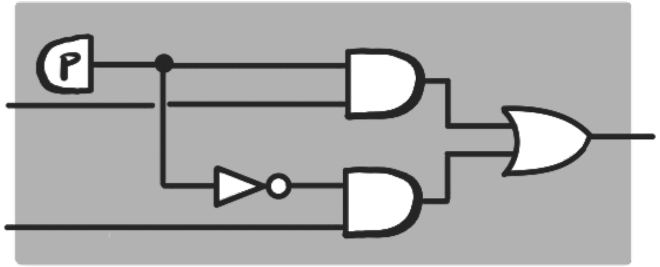
THE ALGEBRA OF PROBABILISTIC BOOLEAN CIRCUITS

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

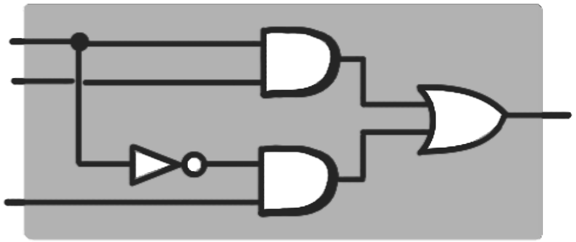
A Complete Axiomatisation of Equivalence for Discrete Probabilistic Programs, ESOP '25

arXiv: 2408.14701

QUESTION

syntax ? semantics ?
equational theory ?

Boolean circuits + Randomness = ?



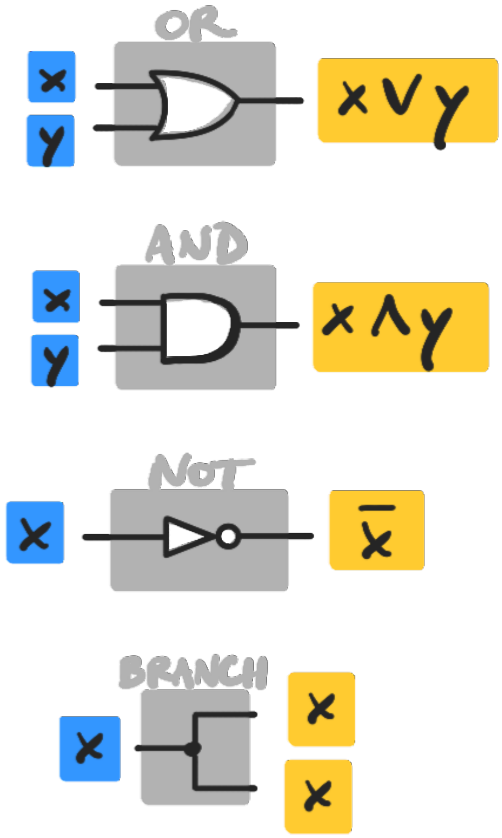
OUTLINE

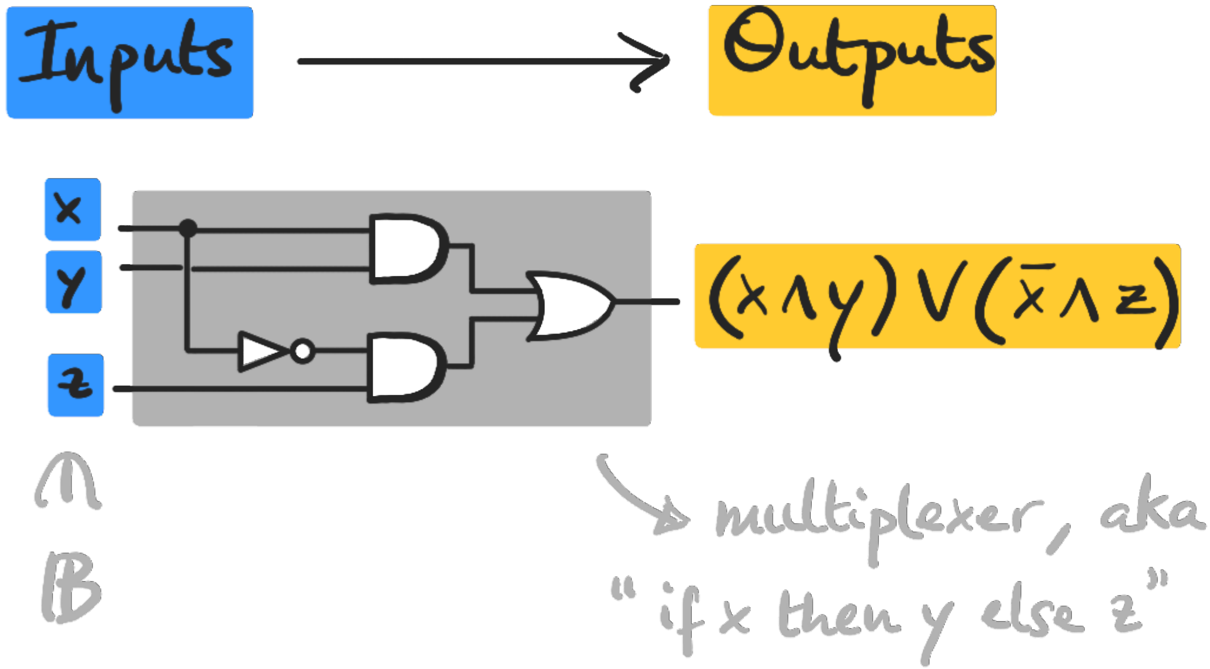
1. BOOLEAN CIRCUITS (PROP-style)
2. PROBABILISTIC BOOLEAN CIRCUITS
3. PROBABILISTIC (BOOLEAN) PROGRAMMING
4. CONCLUSION

OUTLINE

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

BOOLEAN CIRCUITS





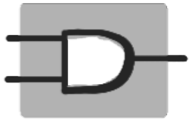
BOOLEAN CIRCUITS

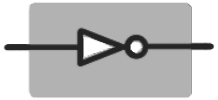
Functorial semantics

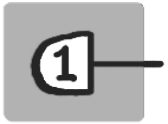
Symmetric monoidal functor

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

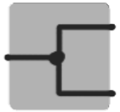
$\underline{\mathrm{BoolCirc}}$ = Free PROP generated by (e.g.)

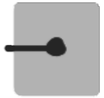
 $\xmapsto{[\![-]\!]}$ $\mathbb{B}^2 \ni (x, y) \mapsto x \wedge y$

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



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

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

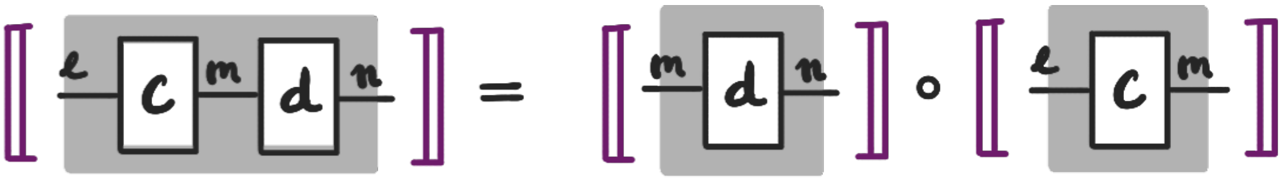
 $\xmapsto{[\![-]\!]}$ $\mathbb{B} \ni x \mapsto \bullet$

BOOLEAN CIRCUITS

Functorial semantics

Symmetric monoidal functor

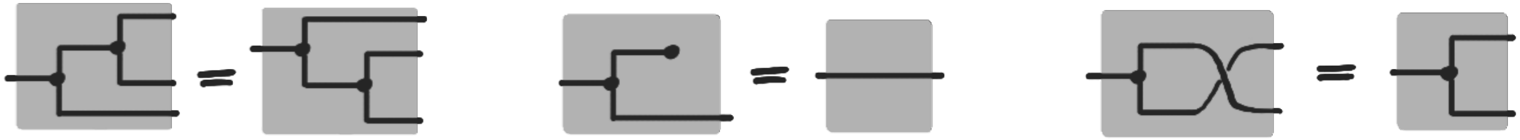
$$\underline{\mathsf{BoolCirc}} \xrightarrow{[\![-]\!]} (\underline{\mathsf{Set}}_{\mathbb{B}}, \times, 1)$$



BOOLEAN CIRCUITS

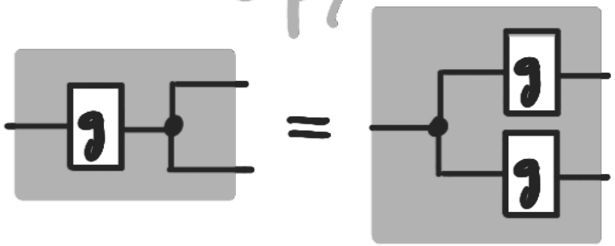
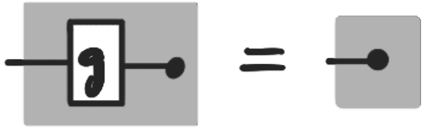
Equational theory

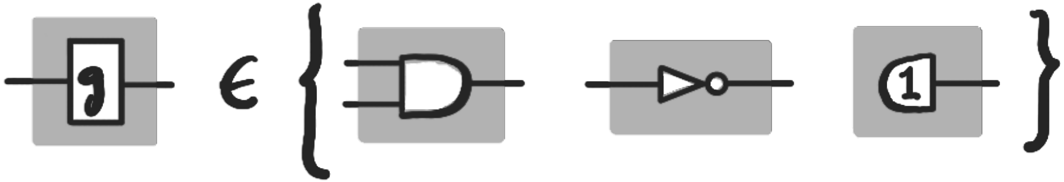
Axioms of Boolean algebra [Boole, 1850s]

+ 

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 $[\![-]\!]$

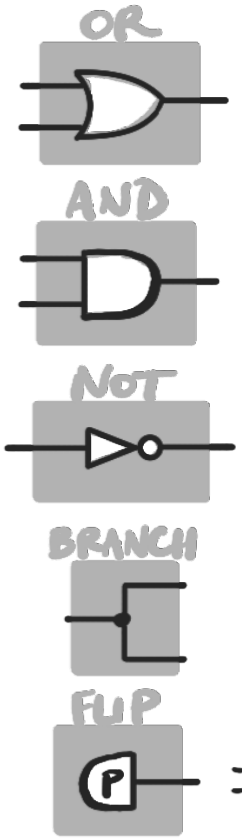
① **Full**: for every $f : \mathbb{B}^m \longrightarrow \mathbb{B}^n$, there exists $\overset{m}{-}\boxed{c}\overset{n}{-}$ s.t. $\left[\!\left[\overset{m}{-}\boxed{c}\overset{n}{-} \right]\!\right] = f$

② **Faithful**: $\left[\!\left[\overset{m}{-}\boxed{c}\overset{n}{-} \right]\!\right] = \left[\!\left[\overset{m}{-}\boxed{d}\overset{n}{-} \right]\!\right] \Rightarrow \overset{m}{-}\boxed{c}\overset{n}{-} = \overset{m}{-}\boxed{d}\overset{n}{-}$

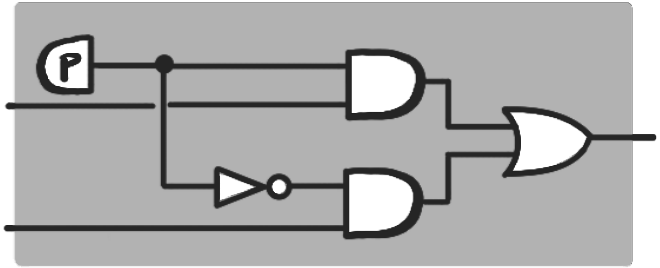
OUTLINE

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

PROBABILISTIC BOOLEAN CIRCUITS



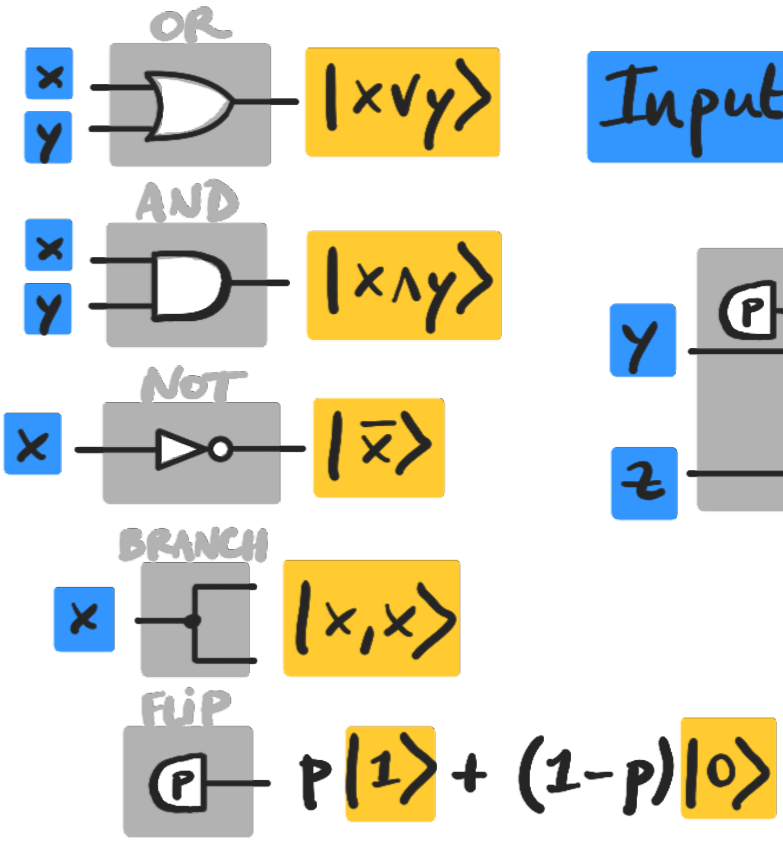
Inputs $\longrightarrow$?



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

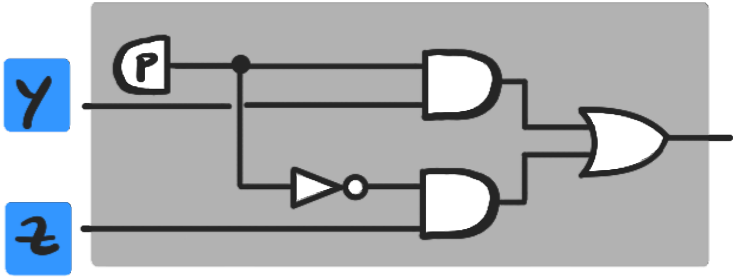
0 with probability $1 - p$

PROBABILISTIC BOOLEAN CIRCUITS



distributions

$$\text{Inputs} \longrightarrow \mathcal{D}(\text{Outputs})$$



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

"p-convex sum of y & z"

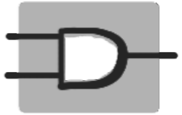
N.B. $|\vec{x}\rangle$ is the Dirac distribution at $\vec{x} \in \mathbb{B}^n$

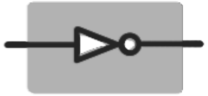
Probabilistic Boolean Circuits

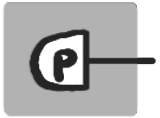
Stochastic maps

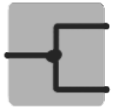
$$\underline{\mathrm{ProbCirc}} \xrightarrow{[\![-]\!]} (\underline{\mathrm{Stoch}}_{\mathbb{B}}, \times, 1)$$

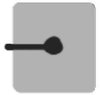
$\underline{\mathrm{ProbCirc}}$ = Free PROP generated by

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

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

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

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

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

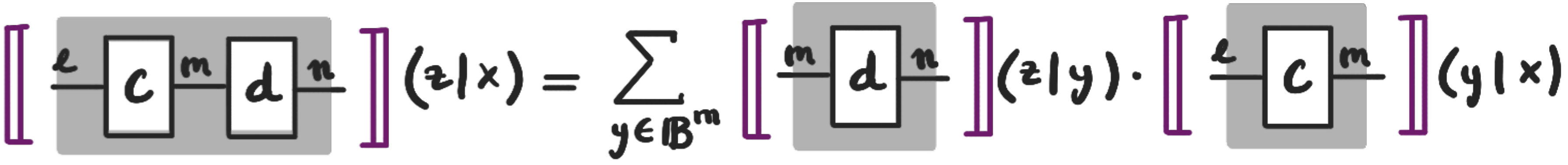
only distribution on one element

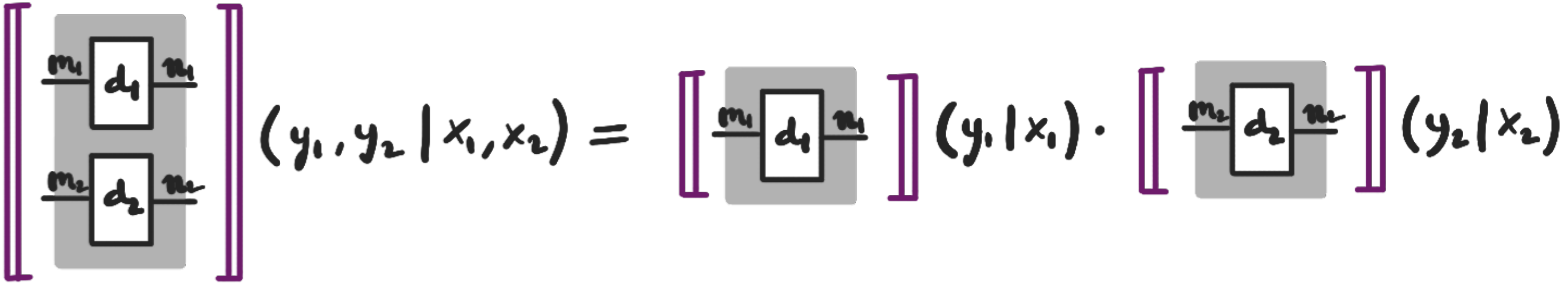
PROBABILISTIC BOOLEAN CIRCUITS

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

Symmetric monoidal functor

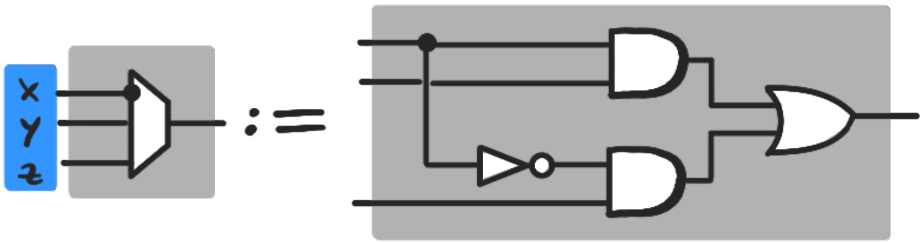
Stochastic maps



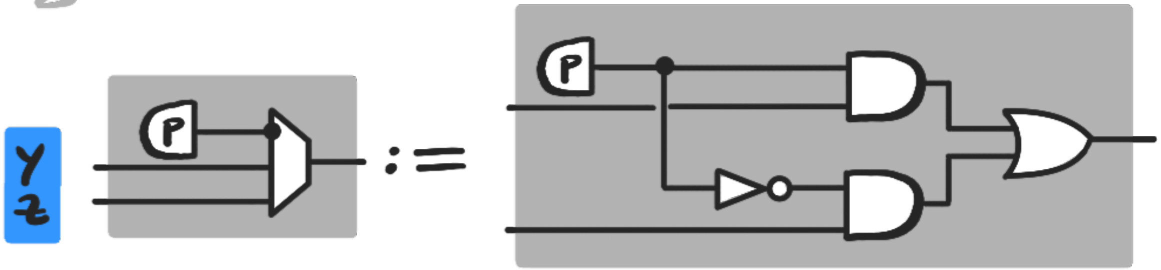


NOTATION

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



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



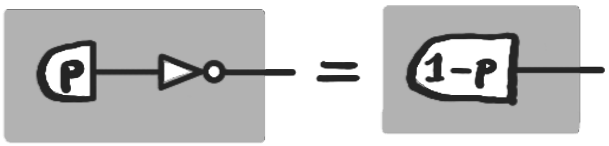
$$p|y\rangle + (1-p)|z\rangle$$

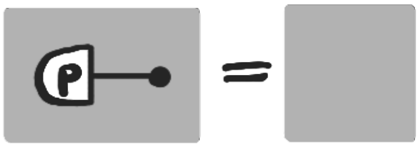
"p-convex sum of y & z"

PROBABILISTIC BOOLEAN CIRCUITS

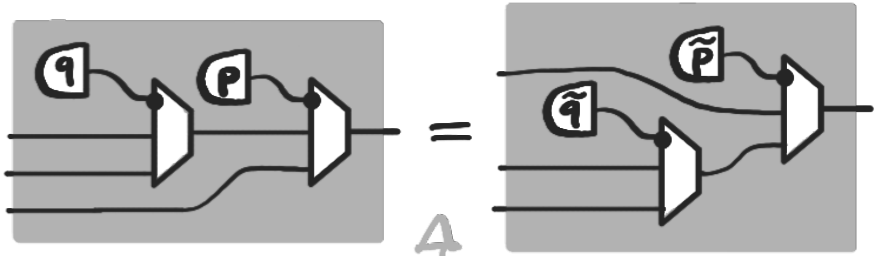
Equational theory (1/3)

Axioms of Boolean circuits +





Bernoulli(p) is a normalised probability dist.



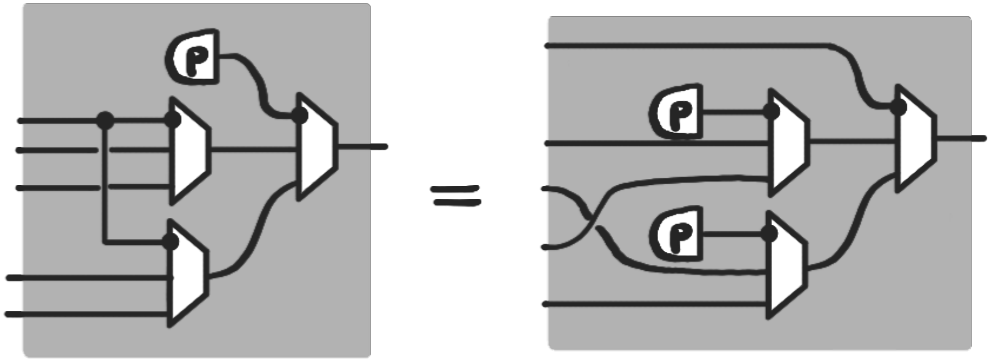
where $\begin{cases} \tilde{p} = pq \\ \tilde{q} = \dfrac{p(1-q)}{1-pq} \end{cases}$ for $pq \neq 1$

M. Stone, Postulates for the barycentric calculus, 1949

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

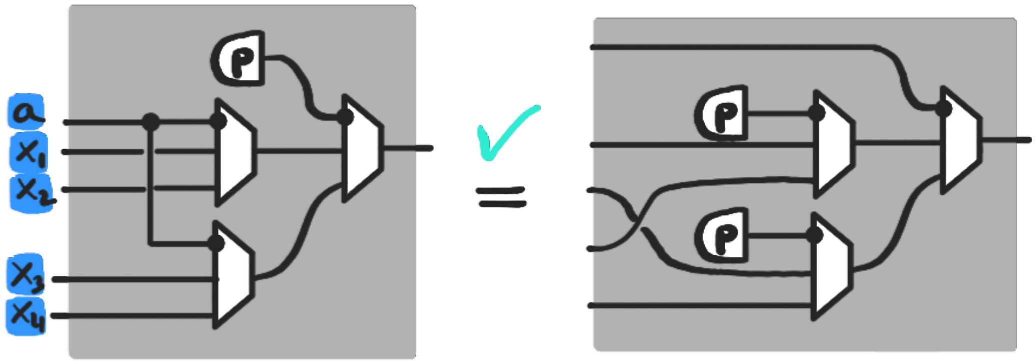
PROBABILISTIC BOOLEAN CIRCUITS

Equational theory (2/3)



Probabilistic Boolean Circuits

Equational theory (2/3)

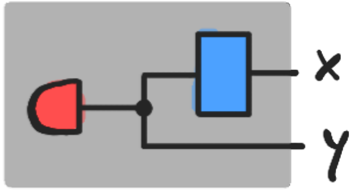


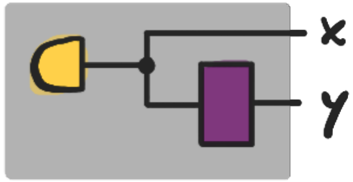
$$\begin{cases} p\,|x_1\rangle + (1-p)\,|x_3\rangle & \text{if } a=1 \\ p\,|x_2\rangle + (1-p)\,|x_4\rangle & \text{if } a=0 \end{cases}$$

PROBABILISTIC BOOLEAN CIRCUITS

Equational theory (3/3)

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





① ②

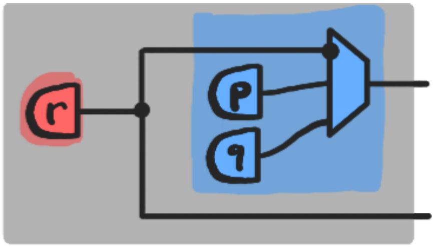
$$p(x,y) = p(x|y)\,p(y) = p(x)\,p(y|x)$$

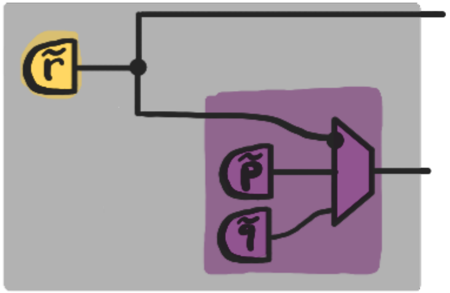
* disintegrate

PROBABILISTIC BOOLEAN CIRCUITS

Equational theory (3/3)

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





① ②

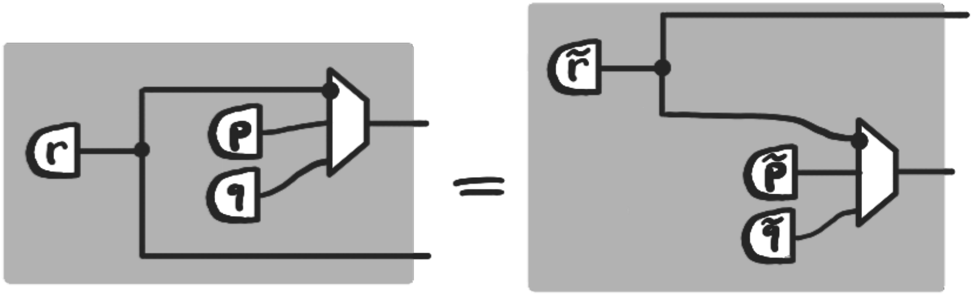
$$p(x,y) = p(x|y)\,p(y) = p(x)\,p(y|x)$$

↳ 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

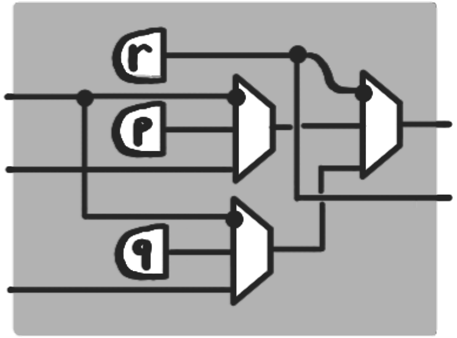
where

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

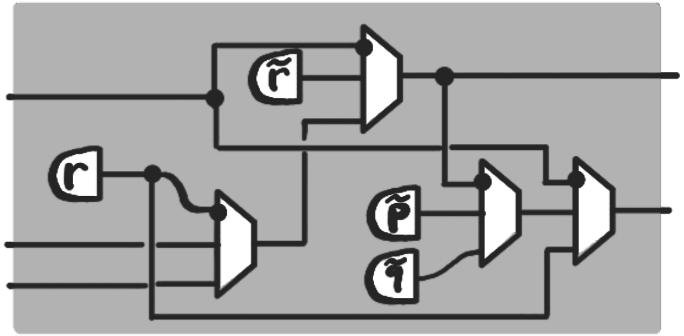
Probabilistic Boolean Circuits

Equational theory (3/3)

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



$=$



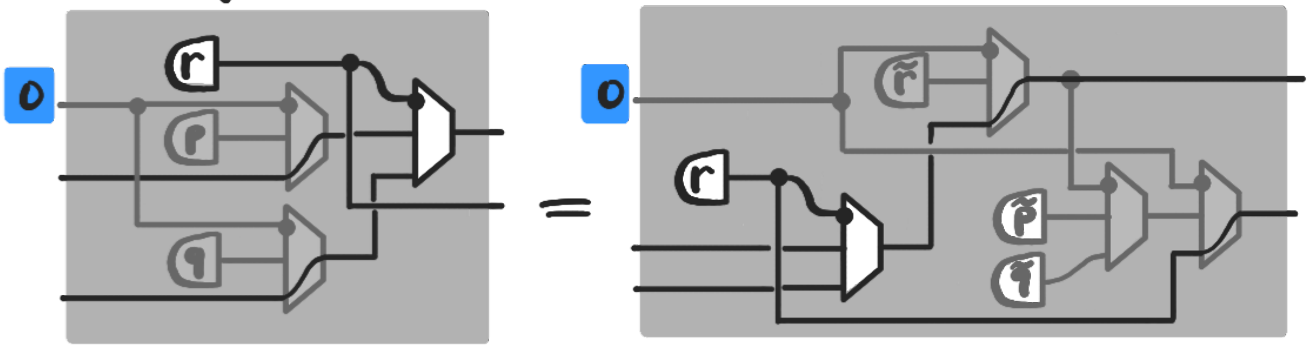
where

$\tilde{r} = rp + (1-r)q$ 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 $\mathbb{B} \times \mathbb{B}$:



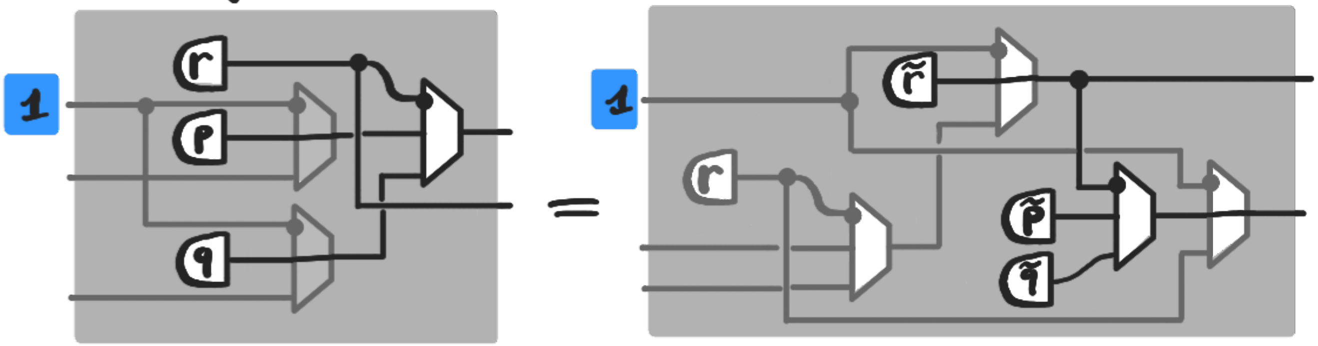
where

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

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

<u>Theorem</u>. The PROP <u>ProbCirc</u> quotiented by the axioms above is <u>isomorphic</u> to the PROP of stochastic maps of type $\mathbb{B}^m \nrightarrow \mathbb{B}^n$.

$[\![-]\!]$

1. <u>Full</u>: for every stochastic map $f : \mathbb{B}^m \nrightarrow \mathbb{B}^n$, there exists $\overset{m}{-}\boxed{c}\overset{n}{-}$ s.t. $[\![\overset{m}{-}\boxed{c}\overset{n}{-}]\!] = f$

2. <u>Faithful</u>: $[\![\overset{m}{-}\boxed{c}\overset{n}{-}]\!] = [\![\overset{m}{-}\boxed{d}\overset{n}{-}]\!] \Rightarrow \overset{m}{-}\boxed{c}\overset{n}{-} = \overset{m}{-}\boxed{d}\overset{n}{-}$

OUTLINE

1. BOOLEAN CIRCUITS (PROP-Style)
2. PROBABILISTIC BOOLEAN CIRCUITS
3. <u>PROBABILISTIC (BOOLEAN) PROGRAMMING</u>
4. CONCLUSION

PROBABILISTIC (BOOLEAN) PROGRAMMING

An example

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

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

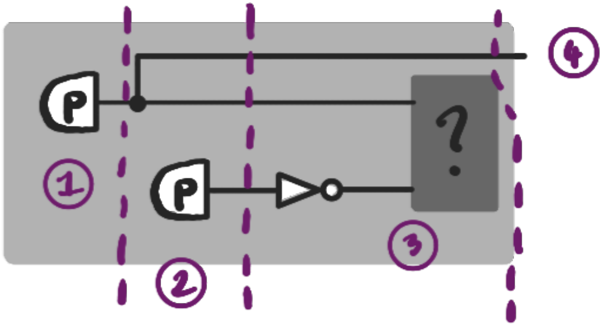
 × 2;

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

Von Neumann's trick

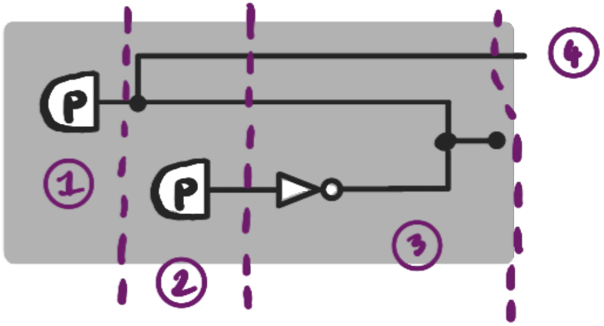


① first = flip p;
② second = flip p;
③ observe (first =! second);
④ return first

PROBABILISTIC (BOOLEAN) PROGRAMMING

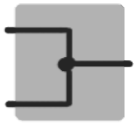
An example

Von Neumann's trick



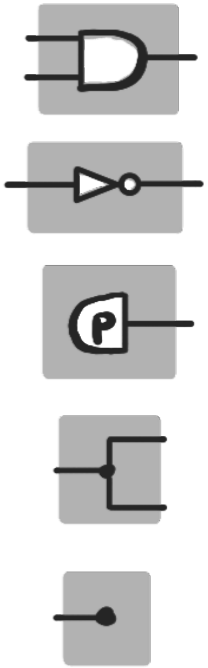
① first = flip p ;
② second = flip p ;
③ observe (first = ! second);
④ return first

where

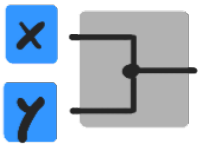
 imposes the condition that its two inputs are equal

PROBABILISTIC (BOOLEAN) PROGRAMMING

Adding first-class conditioning



+

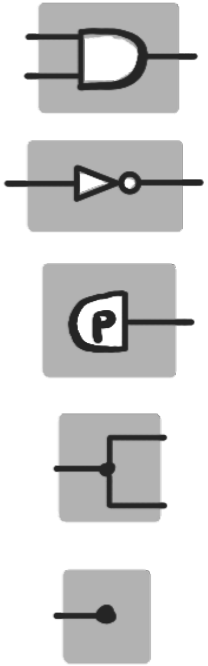


$$\begin{cases} |x\rangle & \text{if } x=y \\ 0 & \text{otherwise} \end{cases}$$

NOT a probability distribution

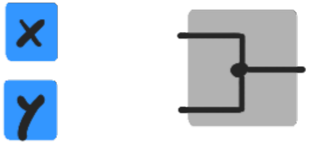
Probabilistic (Boolean) Programming

Adding first-class conditioning



Subdistributions

$$\boxed{\text{Inputs}} \longrightarrow \mathcal{D}_{\leq 1}\left(\boxed{\text{Outputs}}\right)$$

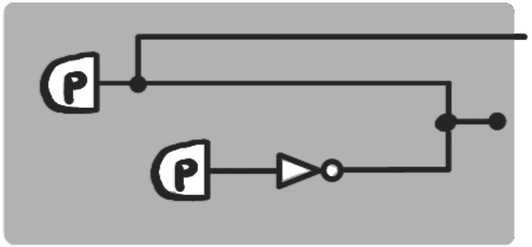


$$\begin{cases} \boxed{|x\rangle} & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$

PROBABILISTIC (BOOLEAN) PROGRAMMING

An example, semantically

Von Neumann's trick



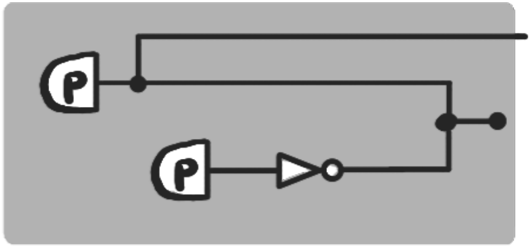
$$\xmapsto{[\![-]\!]} p(1-p)|1\rangle + (1-p)p|0\rangle \neq \frac{1}{2}|1\rangle + \frac{1}{2}|0\rangle$$

in general

PROBABILISTIC (BOOLEAN) PROGRAMMING

An example, semantically

Von Neumann's trick



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

$$\propto$$

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

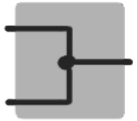
"proportional"

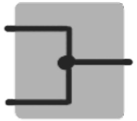
Probabilistic (Boolean) Programming

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 $\times$)

$[\![-]\!]$: ProbCirc +  $\longrightarrow$ (ProjStoch, $\times$, 1)

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

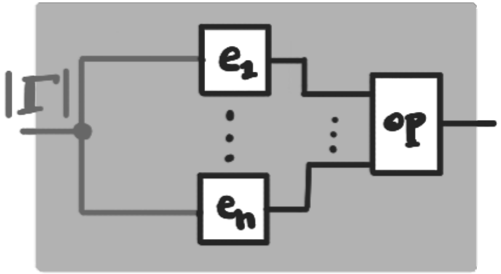
equivalence class

PROBABILISTIC (BOOLEAN) PROGRAMMING

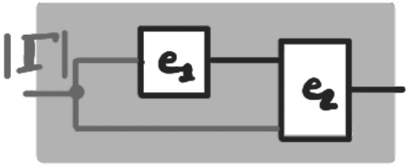
Code as diagrams, diagrams as code

Context = list of free variables

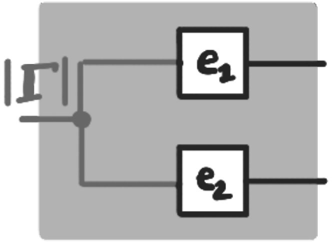
$\Gamma \vdash \mathbf{op}(e_1, \ldots, e_n)$



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

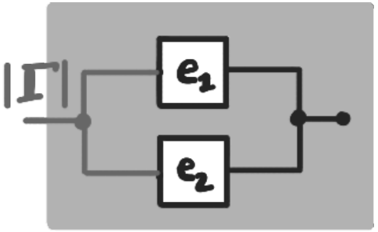


$\Gamma \vdash \langle e_1, e_2 \rangle$



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

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

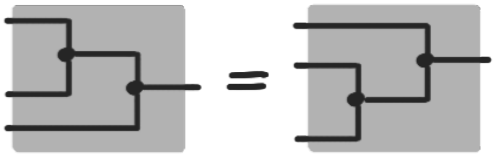


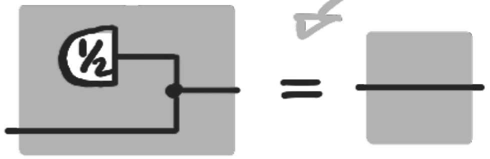
PROBABILISTIC (BOOLEAN) PROGRAMMING

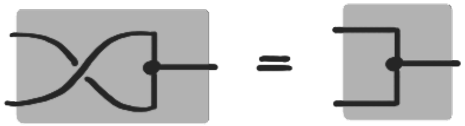
Equational theory (1/2)

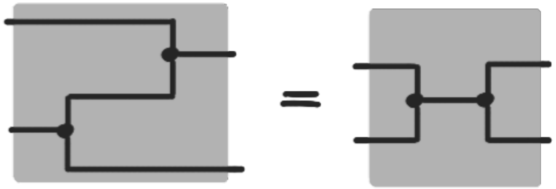
Axioms of probabilistic circuits +

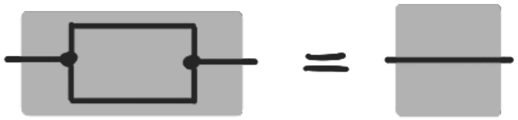
only valid up to $\propto$







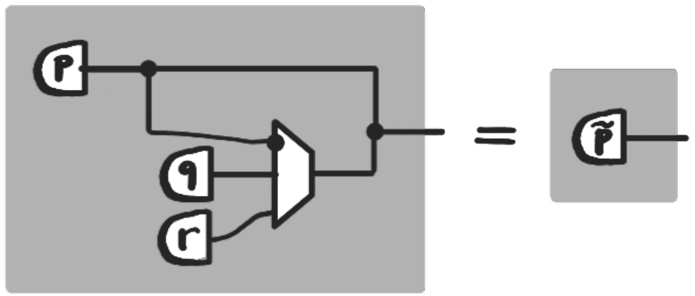




(special Frobenius algebra)

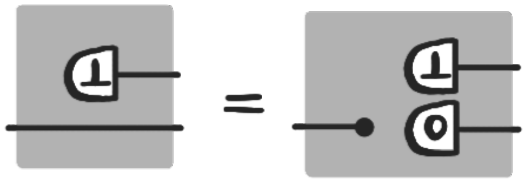
PROBABILISTIC (BOOLEAN) PROGRAMMING

Equational theory (2/2)

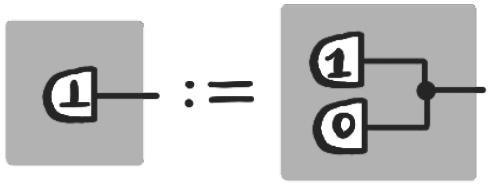


$$\tilde{p} := \frac{pq}{pq + (1-p)(1-r)}$$

↪ if nonzero



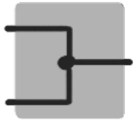
where



failure, aka the zero subdistribution

PROBABILISTIC (BOOLEAN) PROGRAMMING

Complete presentation

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

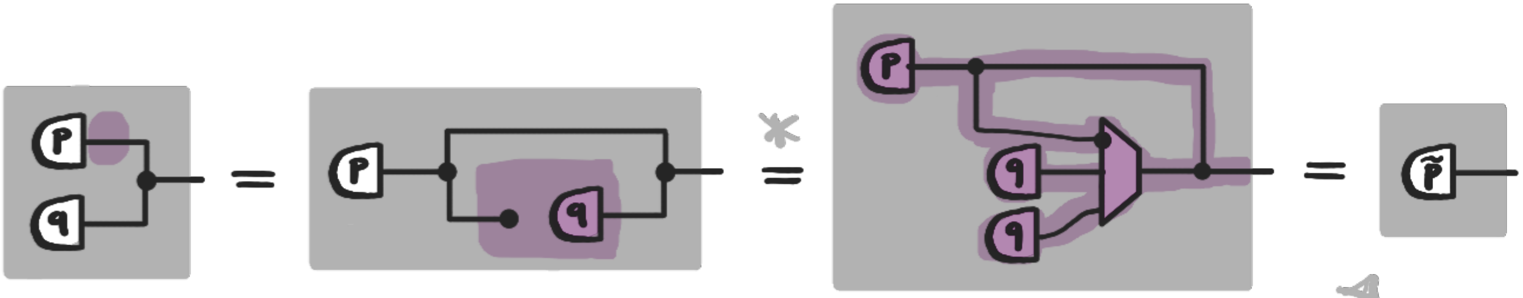
$[\![-]\!]$

① <u>Full</u>: for every substochastic map $f : \mathbb{B}^m \to \mathbb{B}^n$, there exists $m \!-\! \boxed{c} \!-\! n$ s.t. $[\![\, m \!-\! \boxed{c} \!-\! n \,]\!] \propto f$

② <u>Faithful</u>: $[\![\, m \!-\! \boxed{c} \!-\! n \,]\!] \propto [\![\, m \!-\! \boxed{d} \!-\! n \,]\!] \Rightarrow m \!-\! \boxed{c} \!-\! n = m \!-\! \boxed{d} \!-\! n$

VERIFYING VON NEUMANN'S TRICK

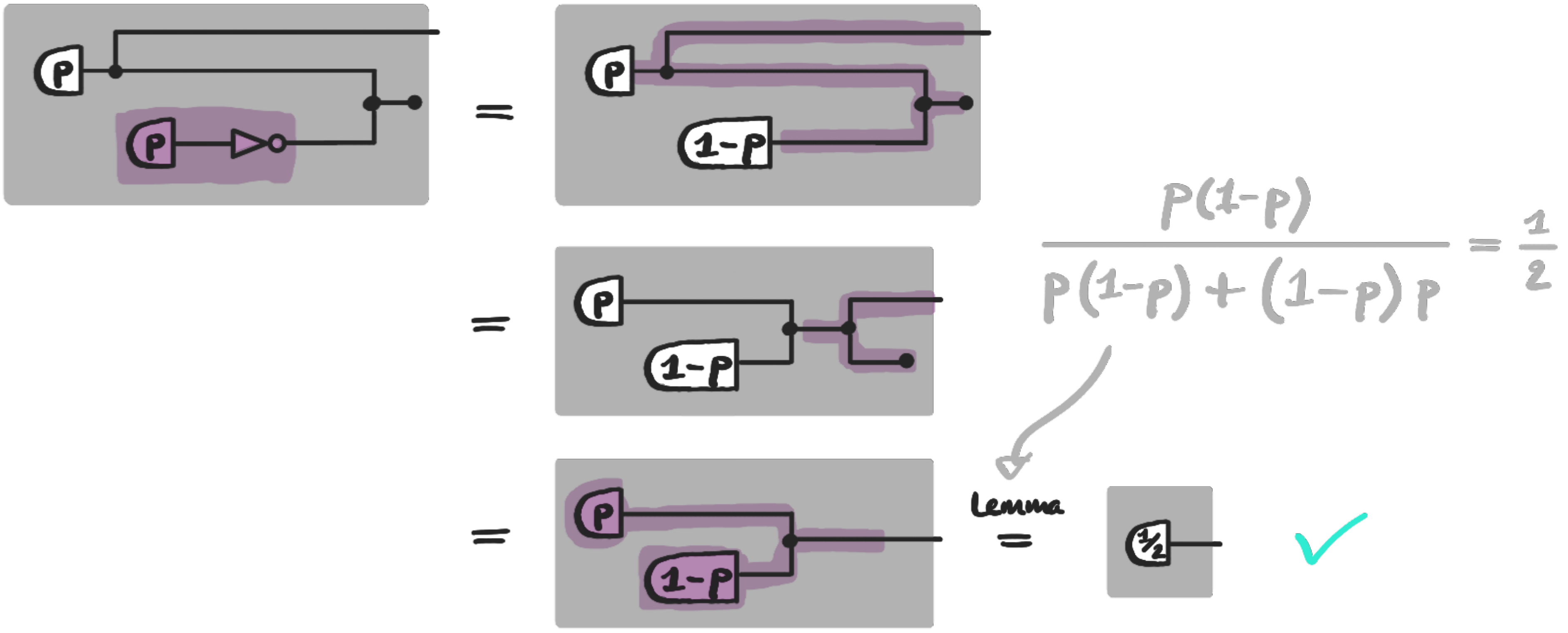
Lemma. For $p, q \in (0,1)$



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

* 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 (<u>not</u> 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