Optics are Monoidal Context

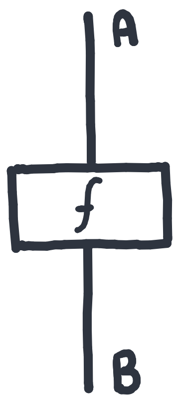
Mario Román joint with Matt Earnshaw and James Hefford

MFPS, 23rd June

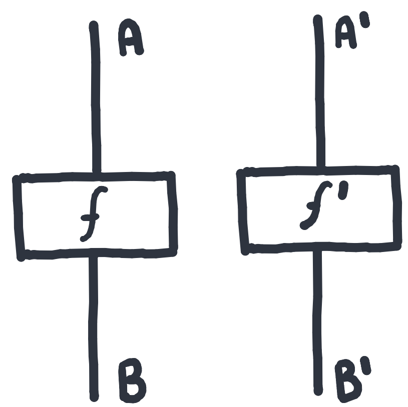
Supported by the EU Estonian IT Academy.

Monoidal Categories: Process Theories

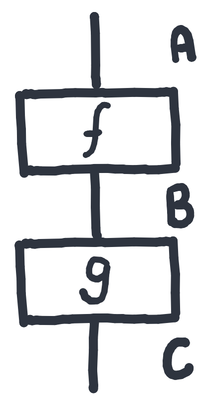
Monoidal categories are an algebra of parallel and sequential composition.
String diagrams are an internal language of monoidal categories.



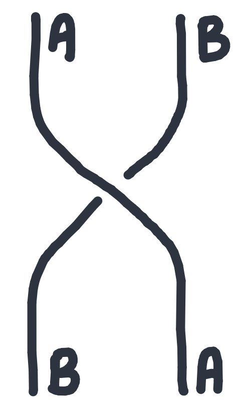
Process



Parallel composition



Sequential composition

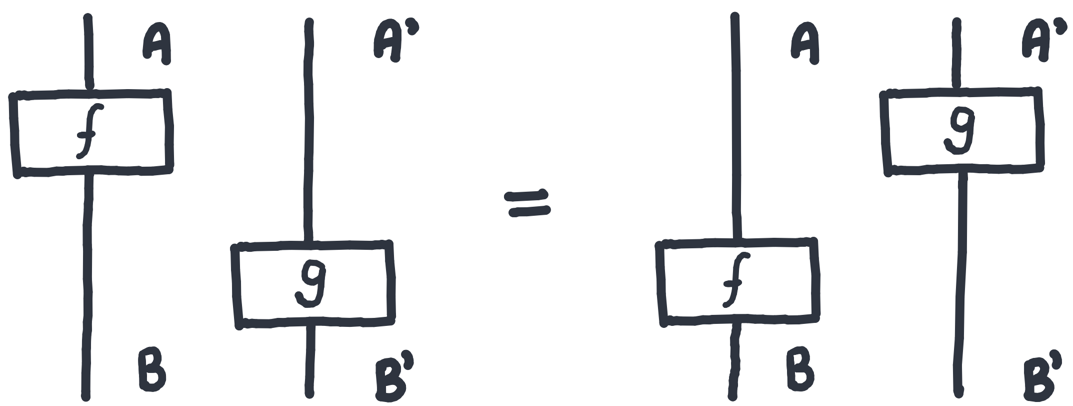


Swap

Bènabou

Monoidal Categories: Process Theories

Monoidal categories are an algebra of parallel and sequential composition.
String diagrams are an internal language of monoidal categories.



Interchange Law

Bènabou

PART 0: Optics

OPTICS

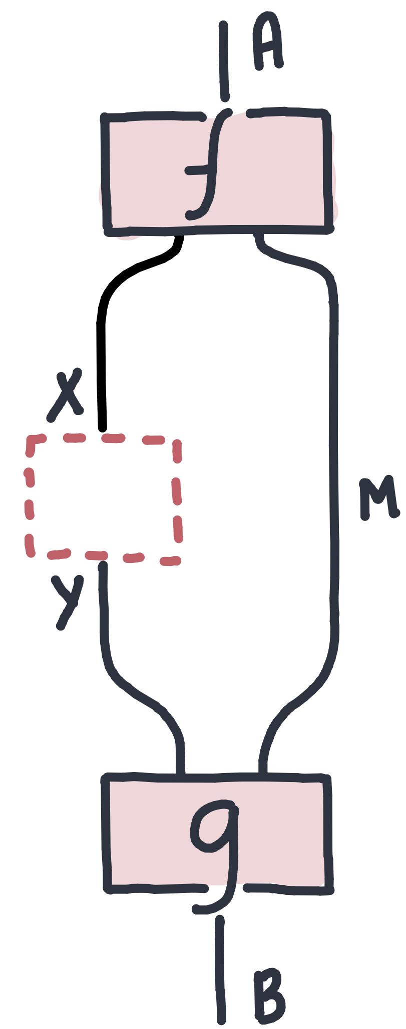
DEFINITION. Let $\mathbb{C}, \otimes, I$ symm. monoidal.

An optic from A to B with a hole from X to Y is a pair of morphisms

$$f : A \to X \otimes M, \qquad g : Y \otimes M \to B,$$

written as $\langle f \mid g \rangle$, and quotiented by dinaturality on M:

$$\langle f ⨾ (id \otimes h) \mid g \rangle = \langle f \mid (id \otimes h) ⨾ g \rangle.$$



OPTICS

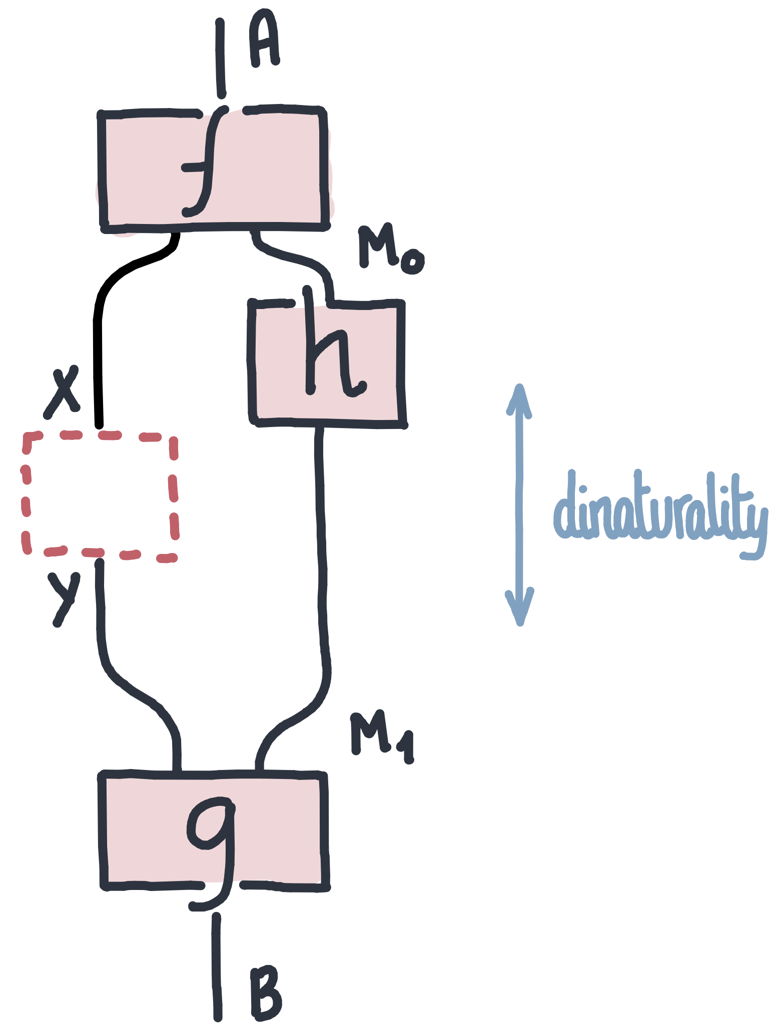
DEFINITION. Let $\mathbb{C}, \otimes, I$ symm. monoidal.

An optic from A to B with a hole from X to Y is a pair of morphisms

$$f : A \to X \otimes M, \qquad g : Y \otimes M \to B,$$

written as $\langle f \mid g \rangle$, and quotiented by dinaturality on M:

$$\langle f ; (id \otimes h) \mid g \rangle = \langle f \mid (id \otimes h) ; g \rangle.$$



OPTICS

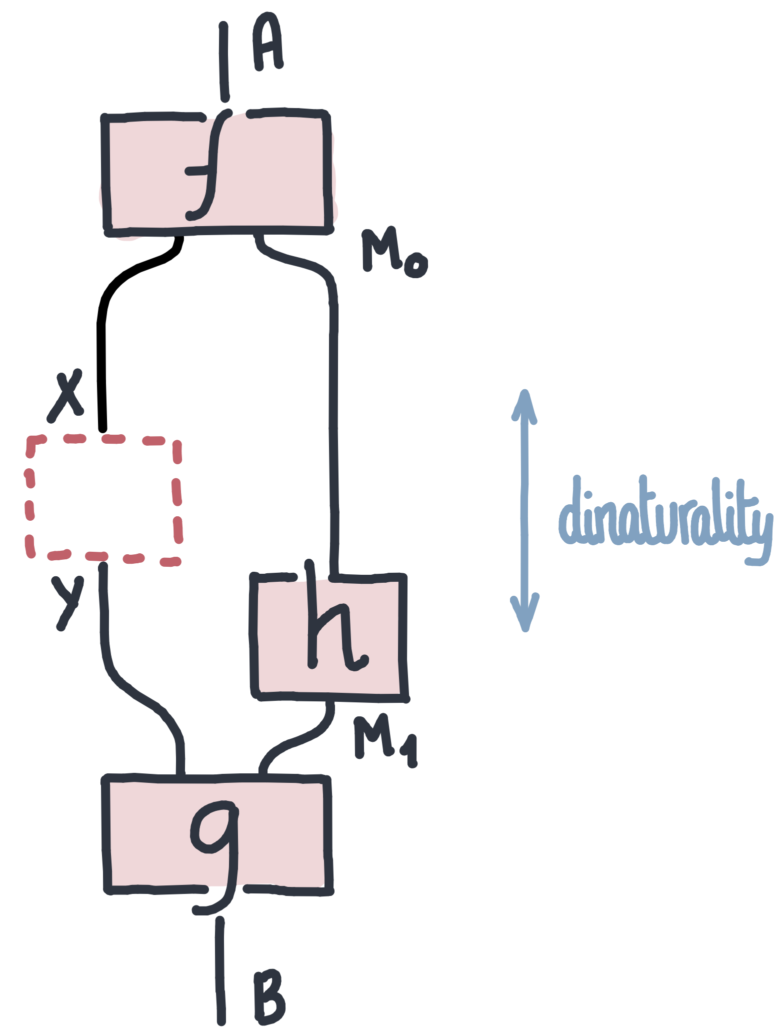
DEFINITION. Let $\mathcal{C}, \otimes, I$ symm. monoidal.

An optic from A to B with a hole from X to Y is a pair of morphisms

$$f : A \to X \otimes M, \qquad g : Y \otimes M \to B,$$

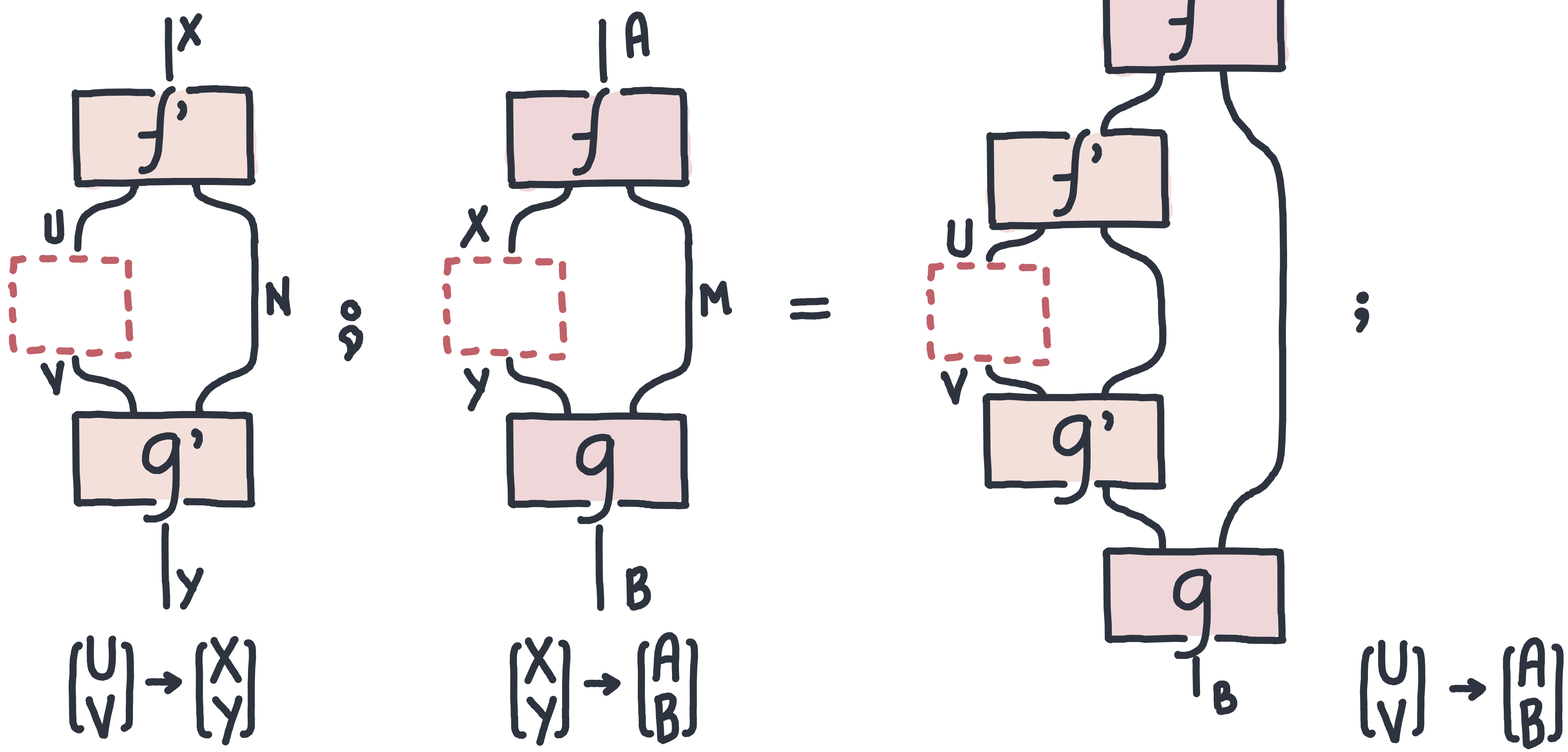
written as $\langle f \mid g \rangle$, and quotiented by dinaturality on M:

$$\langle f ⨾ (id \otimes h) \mid g \rangle = \langle f \mid (id \otimes h) ⨾ g \rangle.$$



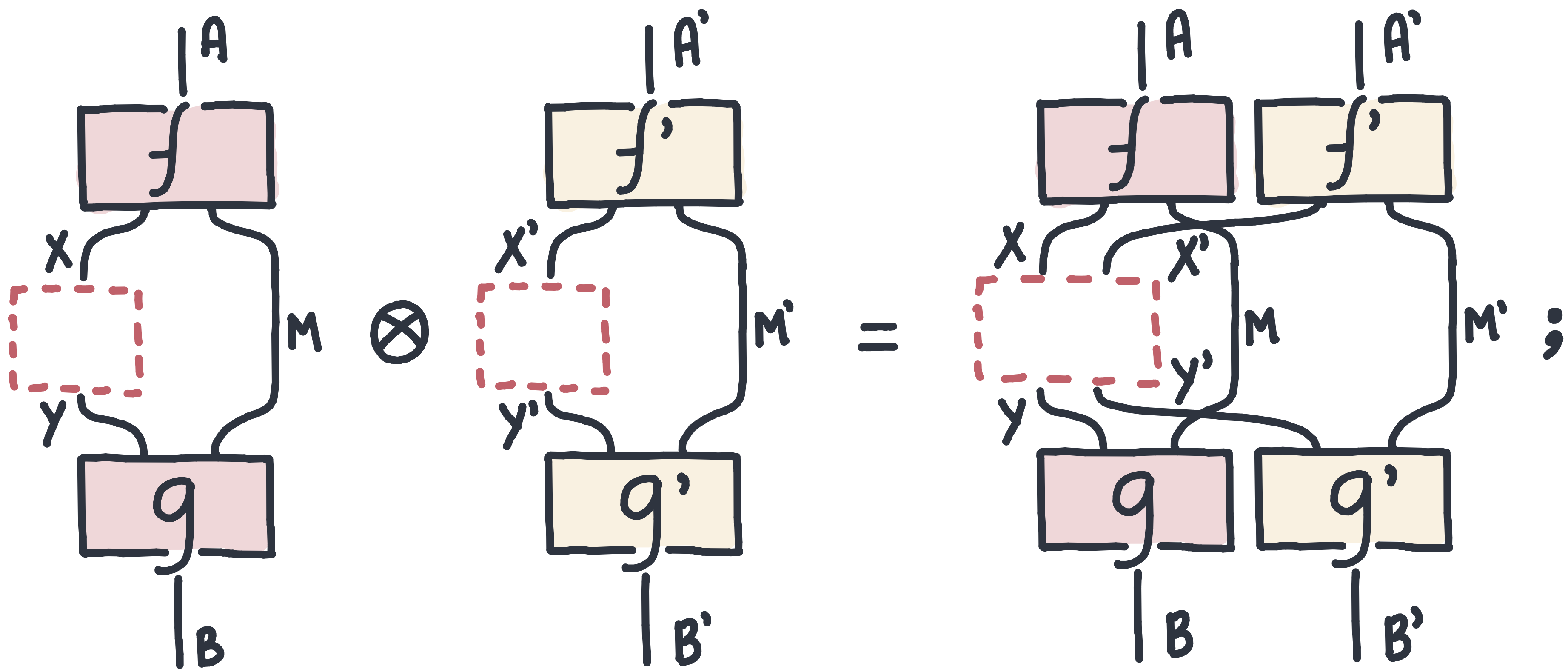
Optics form a Category

Objects are pairs $\begin{bmatrix} X \\ Y \end{bmatrix}$. Composition is



Optics form a Monoidal Category

Tensoring is $\begin{bmatrix} X \\ Y \end{bmatrix} \otimes \begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} X \otimes X' \\ Y \otimes Y' \end{bmatrix}$, and



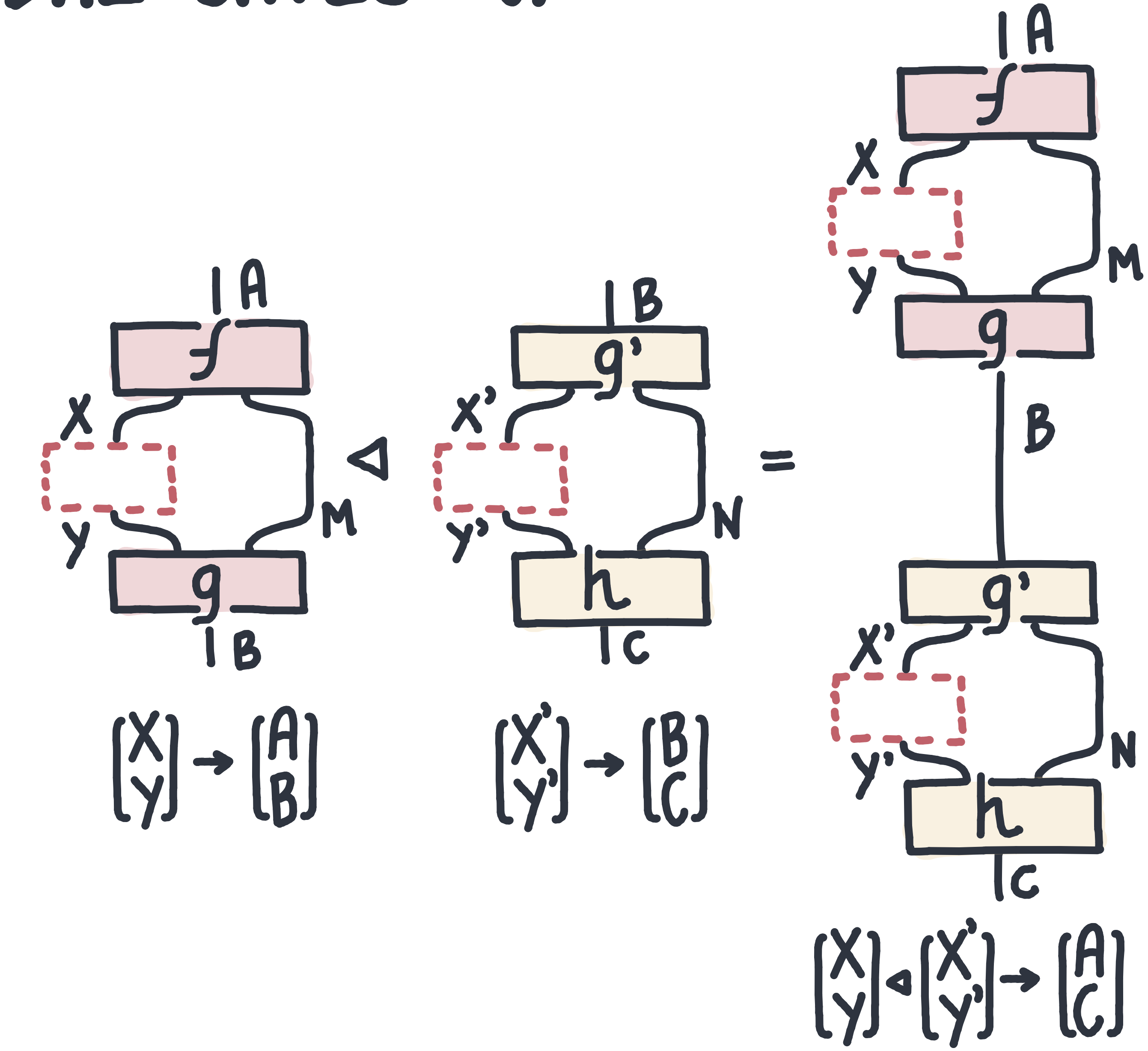
$\begin{bmatrix} X \\ Y \end{bmatrix} \to \begin{bmatrix} A \\ B \end{bmatrix}$ $\quad$ $\begin{bmatrix} X \\ Y \end{bmatrix} \to \begin{bmatrix} A \\ B \end{bmatrix}$ $\quad$ $\begin{bmatrix} X \otimes X' \\ Y \otimes Y' \end{bmatrix} \to \begin{bmatrix} A \otimes A' \\ B \otimes B' \end{bmatrix}$

Optics form a Duoidal Category?

Sequencing is not an operation:

$\begin{bmatrix} X \\ Y \end{bmatrix} \triangleleft \begin{bmatrix} X' \\ Y' \end{bmatrix}$ is not an object, even when $\begin{bmatrix} X \\ Y \end{bmatrix} \triangleleft \begin{bmatrix} X' \\ Y' \end{bmatrix} \to \begin{bmatrix} A \\ B \end{bmatrix}$ is defined.

This is not monoidal, but it is still promonoidal.

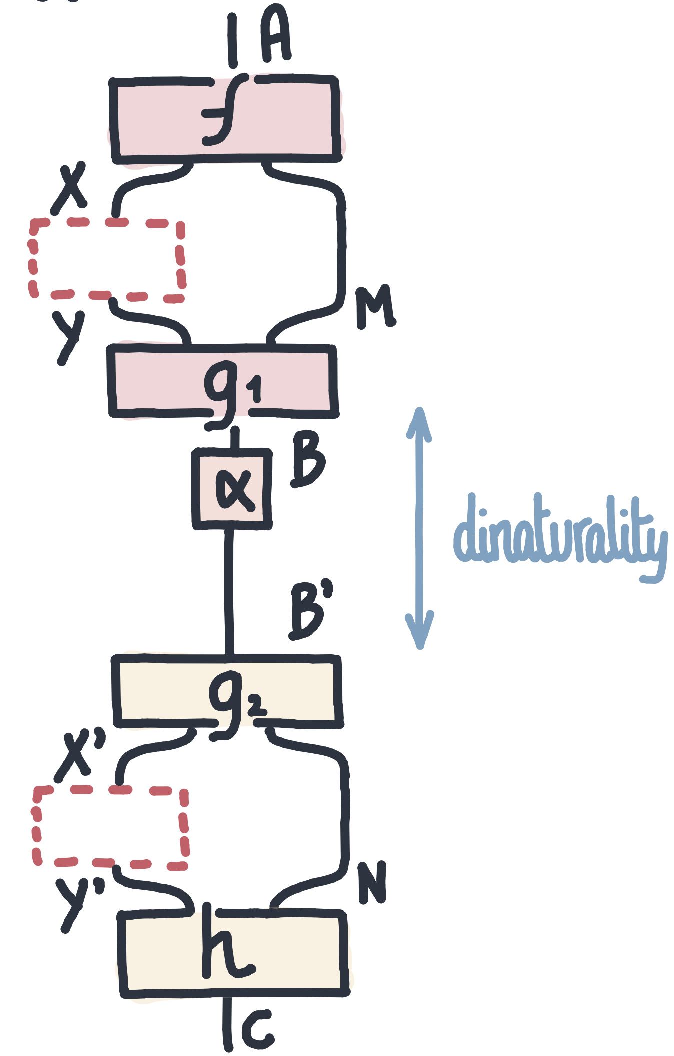


Optics form a Duoidal Category?

Sequencing is not an operation, it defines a hom-set to an object that does not really exist.

$\begin{bmatrix}X\\Y\end{bmatrix} \triangleleft \begin{bmatrix}X'\\Y'\end{bmatrix}$ is not an object,
but $\begin{bmatrix}X\\Y\end{bmatrix} \triangleleft \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix}$ is defined.

This is not monoidal, but it is still promonoidal.



$$\begin{bmatrix}X\\Y\end{bmatrix} \triangleleft \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\C\end{bmatrix}$$

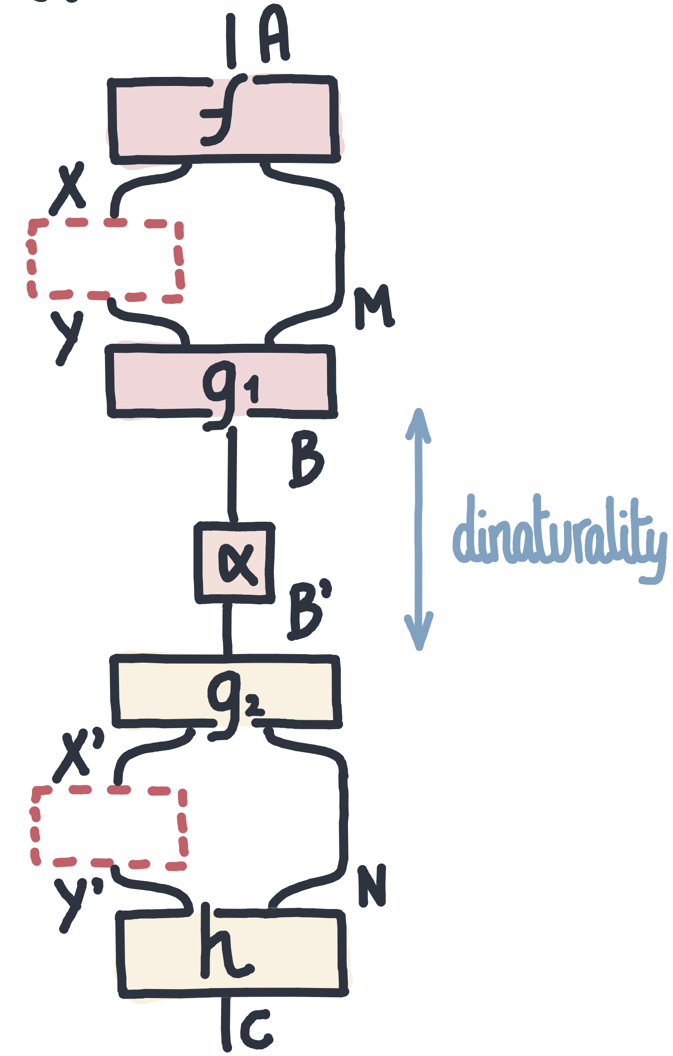
Optics form a Duoidal Category?

Sequencing is not an operation, it defines a hom-set to an object that does not really exist.

$\begin{bmatrix}X\\Y\end{bmatrix} \triangleleft \begin{bmatrix}X'\\Y'\end{bmatrix}$ is not an object,

but $\begin{bmatrix}X\\Y\end{bmatrix} \triangleleft \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix}$ is defined.

This is not monoidal, but it is still promonoidal.



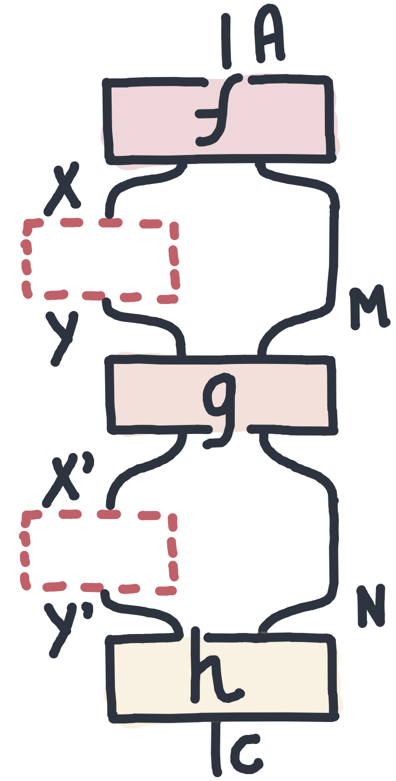
$$\begin{bmatrix}X\\Y\end{bmatrix} \triangleleft \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\C\end{bmatrix}$$

Optics form a Duoidal Category?

Sequencing is not an operation, it defines a hom-set to an object that does not really exist.

$\begin{bmatrix} X \\ Y \end{bmatrix} \triangleleft \begin{bmatrix} X' \\ Y' \end{bmatrix}$ is not an object,
but $\begin{bmatrix} X \\ Y \end{bmatrix} \triangleleft \begin{bmatrix} X' \\ Y' \end{bmatrix} \to \begin{bmatrix} A \\ B \end{bmatrix}$ is defined.

This is not monoidal, but it is still promonoidal.



$$\begin{bmatrix} X \\ Y \end{bmatrix} \triangleleft \begin{bmatrix} X' \\ Y' \end{bmatrix} \to \begin{bmatrix} A \\ C \end{bmatrix}$$

PART 1 : Promonoidals

Monoidal Category

DEFINITION. A monoidal category is a category $\mathbb{C}$ together with functors

$$(\otimes) : \mathbb{C} \times \mathbb{C} \to \mathbb{C}, \qquad I : \mathbb{1} \to \mathbb{C},$$

and natural isomorphisms

$$\alpha_{A,B,C} : A \otimes (B \otimes C) \to (A \otimes B) \otimes C,$$
$$\lambda_A : I \otimes A \to A,$$
$$\rho_A : A \otimes I \to A,$$

satisfying the pentagon and triangle equations.

By nesting, $X \otimes (Y \otimes Z)$, we mean functor composition,

$$X \otimes (Y \otimes Z) :=$$
$$X \otimes M \text{ where } M = Y \otimes Z.$$

Promonoidal Category

DEFINITION. A promonoidal category is a category $\mathbb{C}$ together with profunctors

$$\mathbb{C}(\bullet \otimes \bullet ; \bullet) \colon \mathbb{C}^{op} \times \mathbb{C} \times \mathbb{C} \to \mathrm{SET}, \qquad \mathbb{C}(I ; \bullet) \colon \mathbb{C}^{op} \to \mathrm{SET},$$

and natural bijections,

$$\alpha_{A,B,C} \colon \mathbb{C}(X \otimes (Y \otimes Z) ; \bullet) \to \mathbb{C}((X \otimes Y) \otimes Z ; \bullet),$$
$$\lambda_A \colon \mathbb{C}(I \otimes X ; \bullet) \to \mathbb{C}(X ; \bullet),$$
$$\rho_A \colon \mathbb{C}(X \otimes I ; \bullet) \to \mathbb{C}(X ; \bullet),$$

satisfying the pentagon and triangle equations.

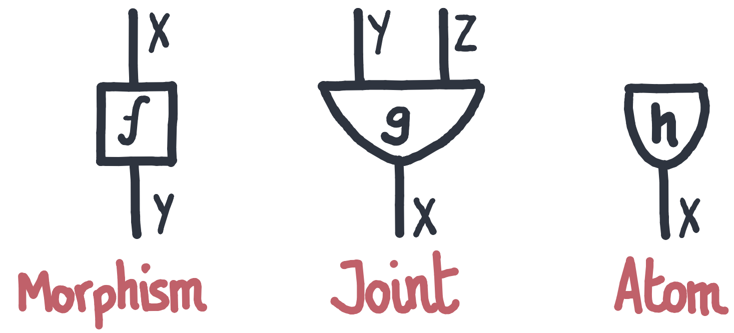
By nesting, $\mathbb{C}(X \otimes (Y \otimes Z) ; \bullet)$, we mean profunctor composition,

$$\mathbb{C}(X \otimes (Y \otimes Z) ; \bullet) := \int^{M} \mathbb{C}(X \otimes M ; \bullet) \times \mathbb{C}(Y \otimes Z ; M).$$

PROMONOIDAL CATEGORIES

Promonoidal categories provide a theory of coherent composition. It has

- Morphisms, $\mathbb{C}(X;A)$.
- Joints, $\mathbb{C}(X \triangleleft Y;A)$.
- Atoms, $\mathbb{C}(N;A)$.

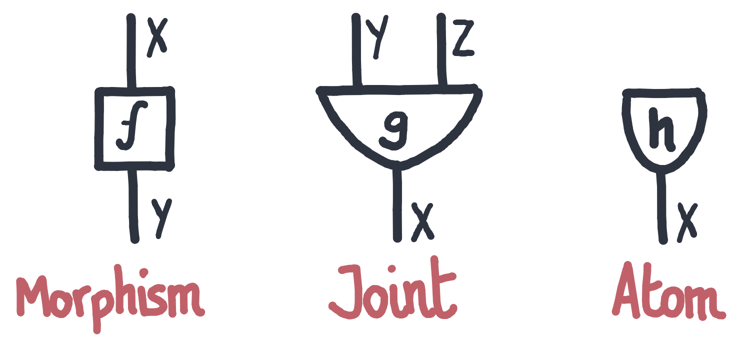


Malleability property: splitting A into X and "something" and then splitting that something into Y and Z can be done in the same number of ways as splitting A into "something" and Z and then splitting that something into X and Y.

PROMONOIDAL CATEGORIES

Promonoidal categories provide a theory of coherent composition. It has

- Morphisms, $\mathbb{C}(X;A)$.
- Joints, $\mathbb{C}(X \triangleleft Y;A)$.
- Atoms, $\mathbb{C}(N;A)$.

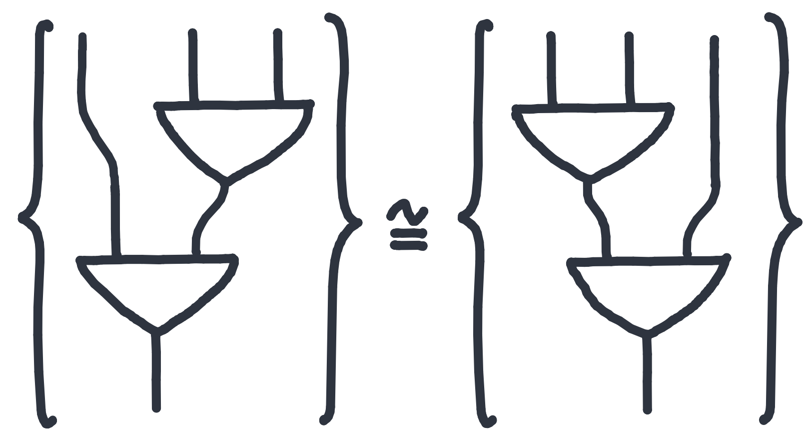


Malleability property:

$$\int^{M\in\mathbb{C}} \mathbb{C}(A;X\otimes M)\times\mathbb{C}(M;Y\otimes Z) \cong \int^{M\in\mathbb{C}} \mathbb{C}(A;M\otimes Z)\times\mathbb{C}(M;X\otimes Y);$$

$$\int^{M\in\mathbb{C}} \mathbb{C}(A;X\otimes M)\times\mathbb{C}(M;I) \cong \mathbb{C}(A;X);$$

$$\int^{M\in\mathbb{C}} \mathbb{C}(A;M\otimes X)\times\mathbb{C}(M;I) \cong \mathbb{C}(A;X);$$



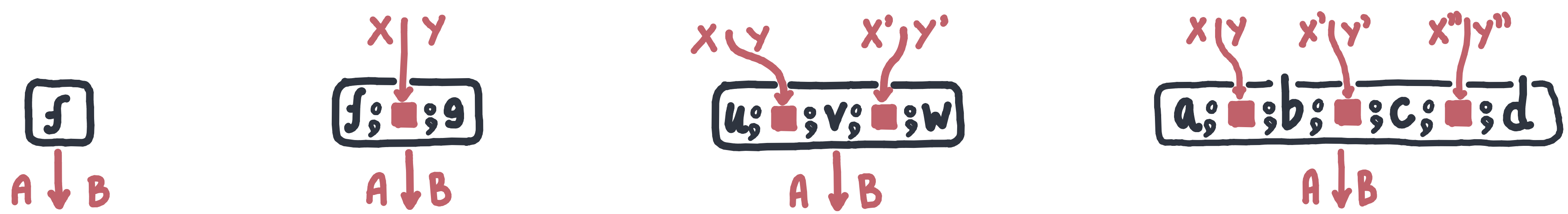
PART 2: Context for Categories

CONTEXT FOR CATEGORIES

Consider 'expressions with holes' in a category, like the following

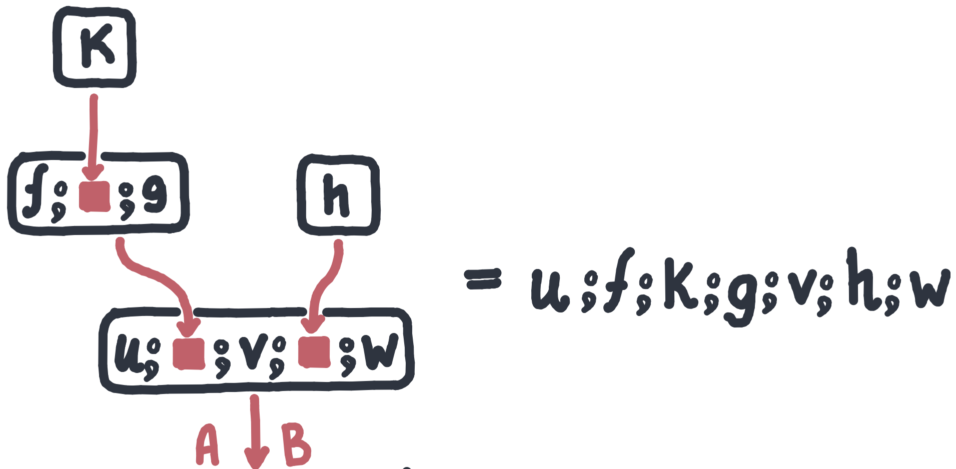
$$u \mathbin{;} \blacksquare \mathbin{;} v \mathbin{;} \blacksquare \mathbin{;} w, \qquad f \mathbin{;} \blacksquare \mathbin{;} g, \qquad f, \qquad a \mathbin{;} \blacksquare \mathbin{;} b \mathbin{;} \blacksquare \mathbin{;} c \mathbin{;} \blacksquare \mathbin{;} d.$$

These contexts form a promonoidal category.

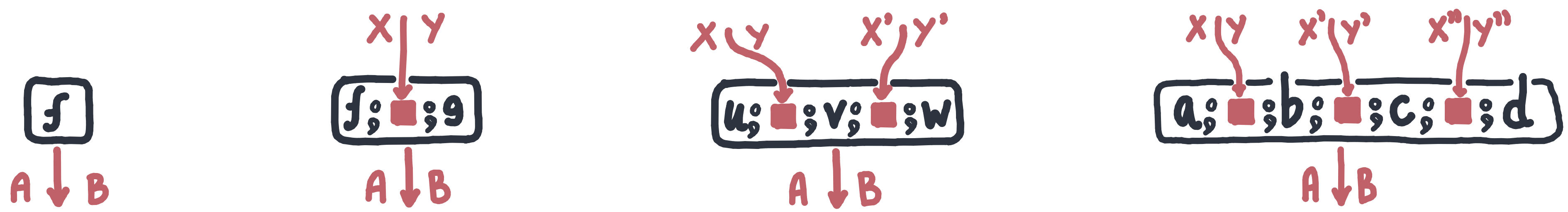


$$\begin{bmatrix}A\\B\end{bmatrix} \qquad \begin{bmatrix}X\\Y\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix} \qquad \begin{bmatrix}X\\Y\end{bmatrix} \triangleleft \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\C\end{bmatrix} \qquad \begin{bmatrix}X\\Y\end{bmatrix} \triangleleft \begin{bmatrix}X'\\Y'\end{bmatrix} \triangleleft \begin{bmatrix}X''\\Y''\end{bmatrix} \to \begin{bmatrix}A\\C\end{bmatrix}$$

CONTEXT FOR CATEGORIES



These contexts form a promonoidal category.



$$\begin{bmatrix} A \\ B \end{bmatrix} \qquad \begin{bmatrix} X \\ Y \end{bmatrix} \to \begin{bmatrix} A \\ B \end{bmatrix} \qquad \begin{bmatrix} X \\ Y \end{bmatrix} \triangleleft \begin{bmatrix} X' \\ Y' \end{bmatrix} \to \begin{bmatrix} A \\ C \end{bmatrix} \qquad \begin{bmatrix} X \\ Y \end{bmatrix} \triangleleft \begin{bmatrix} X' \\ Y' \end{bmatrix} \triangleleft \begin{bmatrix} X'' \\ Y'' \end{bmatrix} \to \begin{bmatrix} A \\ C \end{bmatrix}$$

Contour is Adjoint to Splice

What is a canonical algebra of context on top of a monoidal category?

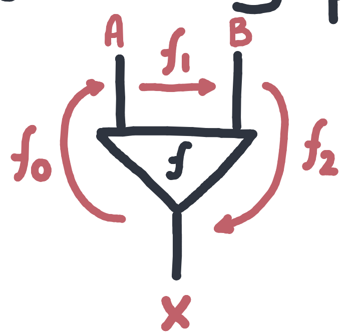
- Each category gives a cofree promonoidal, context.
- Each promonoidal gives a free category, contour.

$$\begin{tikzcd} \text{Category} \arrow[r, bend left, "\text{Context}"] \arrow[r, phantom, "\top"] & \text{Promonoidal Category} \arrow[l, bend left, "\text{Contour}"] \end{tikzcd}$$

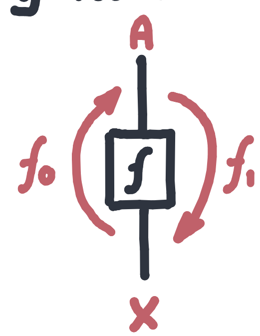
CONTOUR

Meliès, Zeilberger.

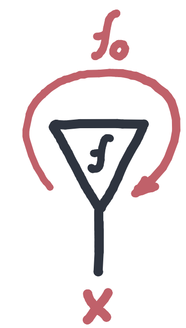
Contouring promonoidal categories generates a category.



$$f_0 : X^L \to A^L$$
$$f_1 : A^R \to B^L$$
$$f_2 : B^R \to X^R$$

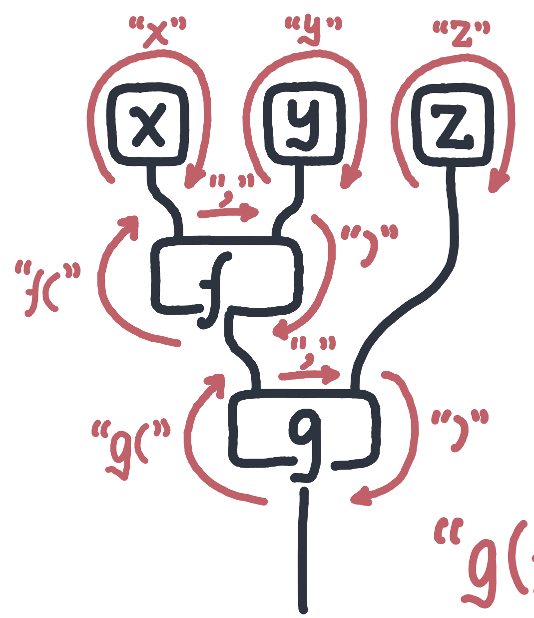


$$f_0 : X^L \to A^L$$
$$f_1 : A^R \to X^R$$



$$f_0 : X^L \to X^R.$$

The category provides
a simple parsing algebra to
any promonoidal,
or any multicategory.



"g(f(x,y),z)"

Next

$$
\begin{tikzcd}
\text{Monoidal Category} \arrow[r, bend left, "\text{Mon. Context}"] \arrow[r, phantom, "\top"] \arrow[d] & \text{Produoidal Category} \arrow[l, bend left, "\text{Mon. Contour}"] \arrow[d] & \\
\text{Category} \arrow[r, bend left, "\text{Context}"] \arrow[r, phantom, "\top"] & \text{Promonoidal Category} \arrow[l, bend left, "\text{Contour}"] & \text{Duoidal Category} \arrow[ul, dashed]
\end{tikzcd}
$$

Part 4 : Context for Monoidal Categories

Monoidal Context-Contour

What is a canonical algebra of decomposition on top of a monoidal category?

- Each monoidal category gives a cofree produoidal, monoidal context.
- Each produoidal gives a free monoidal category, monoidal contour.

$$
\begin{tikzcd}
\text{Monoidal Category} \arrow[r, bend left, "\text{Monoidal Context}"] \arrow[r, phantom, "\top"] & \text{Produoidal Category} \arrow[l, bend left, "\text{Monoidal Contour}"]
\end{tikzcd}
$$

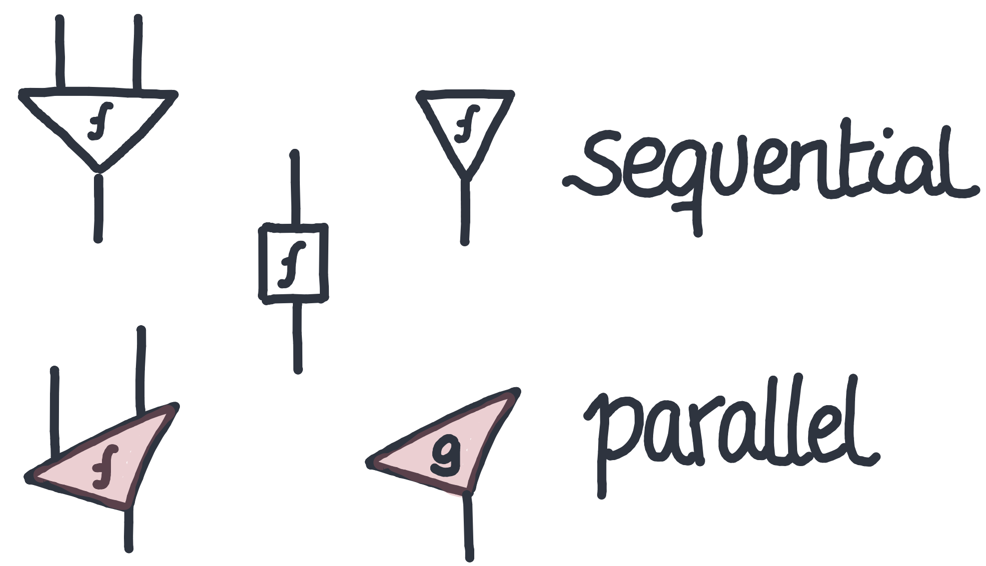
Produoidal Categories

Definition. A produoidal is a pair of promonoidals

$$\mathbb{V}(\bullet \triangleleft \bullet ; \bullet) : \mathbb{V}^{op} \times \mathbb{V} \times \mathbb{V} \to \mathbf{Set}, \quad \mathbb{V}(\bullet ; N) : \mathbb{V}^{op} \to \mathbf{Set}, \quad \text{"sequential"},$$
$$\mathbb{V}(\bullet ; \bullet \otimes \bullet) : \mathbb{V}^{op} \times \mathbb{V} \times \mathbb{V} \to \mathbf{Set}, \quad \mathbb{V}(\bullet ; I) : \mathbb{V}^{op} \to \mathbf{Set}, \quad \text{"parallel"}.$$

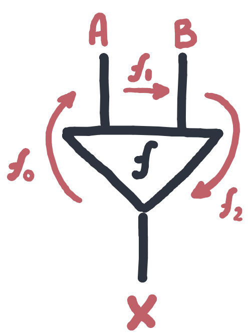
One laxly distributes over the other,

$$\begin{aligned}
\psi_2 &: (A \triangleleft B) \otimes (C \triangleleft D) \longrightarrow (A \otimes C) \triangleleft (B \otimes D), \\
\psi_0 &: I \longrightarrow N \\
\varphi_2 &: N \longrightarrow N \triangleleft N \\
\varphi_0 &: I \longrightarrow I \otimes I
\end{aligned}$$

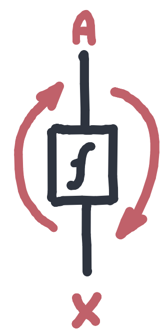


Monoidal Contour

Contouring produoidal categories generates a monoidal category.

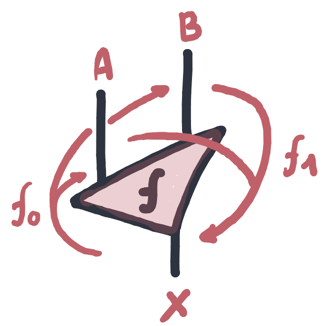


$f_0 : X^L \to A^L$
$f_1 : A^R \to B^L$
$f_2 : B^R \to X^R$

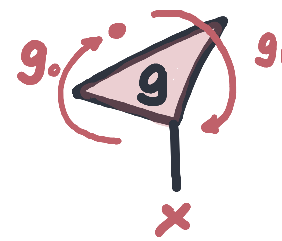


$f_0 : X^L \to A^L$
$f_1 : A^R \to X^R$

$f_0 : X^L \to X^R$



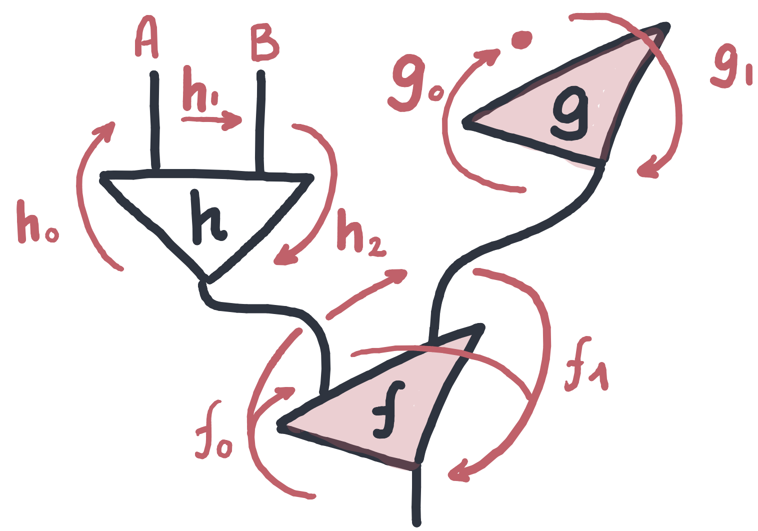
$f_0 : X^L \to A^L \otimes B^L$
$f_1 : A^R \otimes B^R \to X^R$

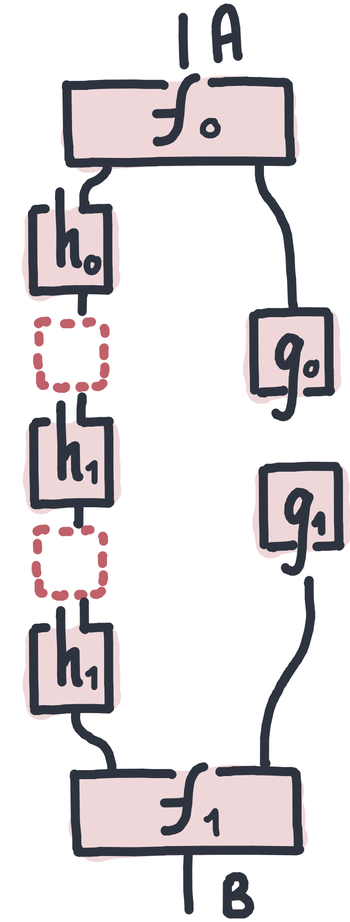


$g_0 : X^L \to I$
$g_1 : I \to X^R$

Monoidal Contour

Contouring produoidal categories generates a monoidal category. Example.



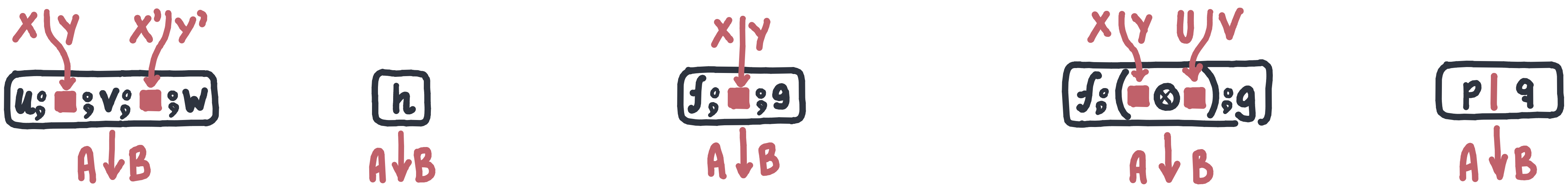


Monoidal Context

Consider 'expressions with holes' in a monoidal category, like the following

$$u ; \blacksquare ; v ; \blacksquare ; w, \qquad k, \qquad f ; (\blacksquare \otimes \blacksquare) ; g, \qquad p \mid q .$$

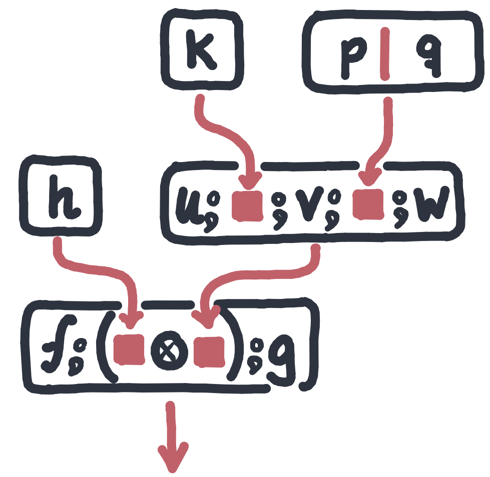
These contexts form a produoidal category.



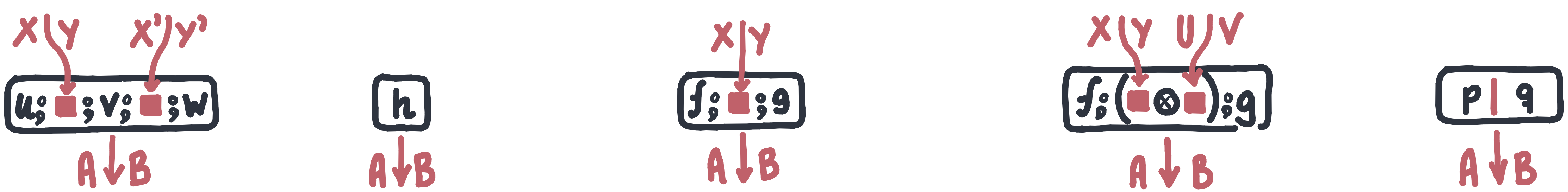
$$\begin{bmatrix}X\\Y\end{bmatrix} \triangleleft \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix} \qquad N \to \begin{bmatrix}A\\B\end{bmatrix} \qquad \begin{bmatrix}X\\Y\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix} \qquad \begin{bmatrix}X\\Y\end{bmatrix} \otimes \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix} \qquad I \to \begin{bmatrix}A\\B\end{bmatrix}$$

Monoidal Context

$$f ; (h \otimes (u ; k ; v ; p ; q ; w)) ; g \quad =$$



These contexts form a produoidal category.



$\begin{bmatrix}X\\Y\end{bmatrix} \triangleleft \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix}$ $\quad N \to \begin{bmatrix}A\\B\end{bmatrix}$ $\quad \begin{bmatrix}X\\Y\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix}$ $\quad \begin{bmatrix}X\\Y\end{bmatrix} \otimes \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix}$ $\quad I \to \begin{bmatrix}A\\B\end{bmatrix}$

Monoidal Context-Contour

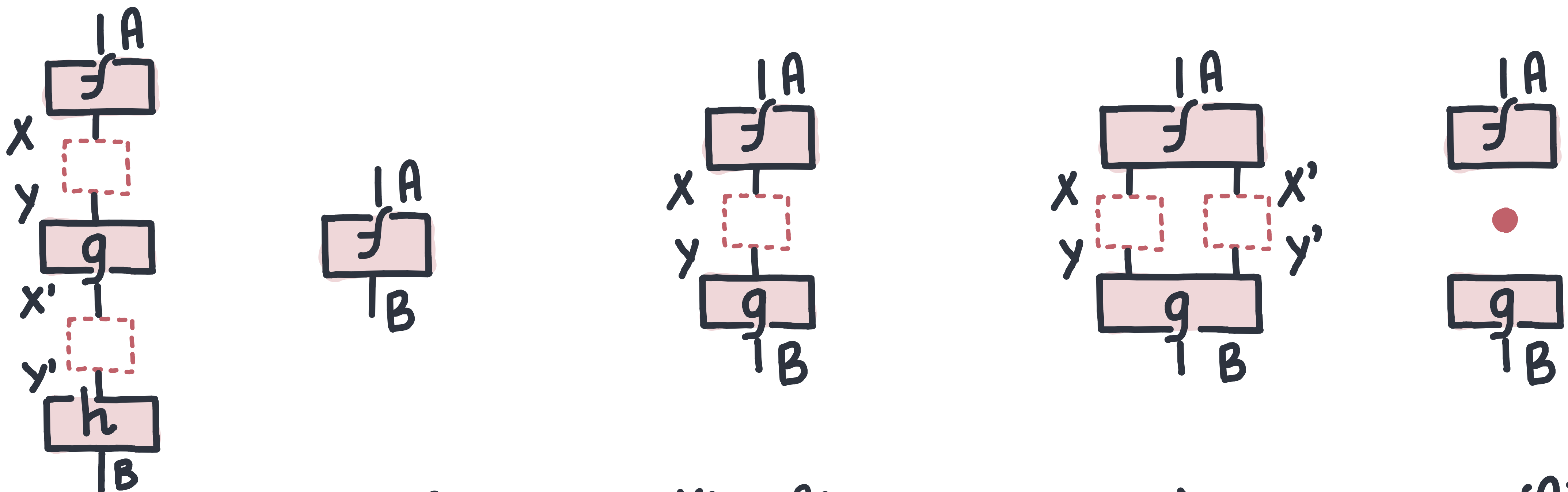
What is a canonical algebra of decomposition on top of a monoidal category?

- Each monoidal category gives a cofree produoidal, monoidal context.
- Each produoidal gives a free monoidal category, monoidal contour.

$$
\begin{tikzcd}
\text{Monoidal Category} \arrow[r, bend left, "\text{Monoidal Context}"] \arrow[r, phantom, "\top"] & \text{Produoidal Category} \arrow[l, bend left, "\text{Monoidal Contour}"]
\end{tikzcd}
$$

Monoidal Context

THM (EHR'23). Spliced monoidal arrows are the cofree produoidal on a monoidal.

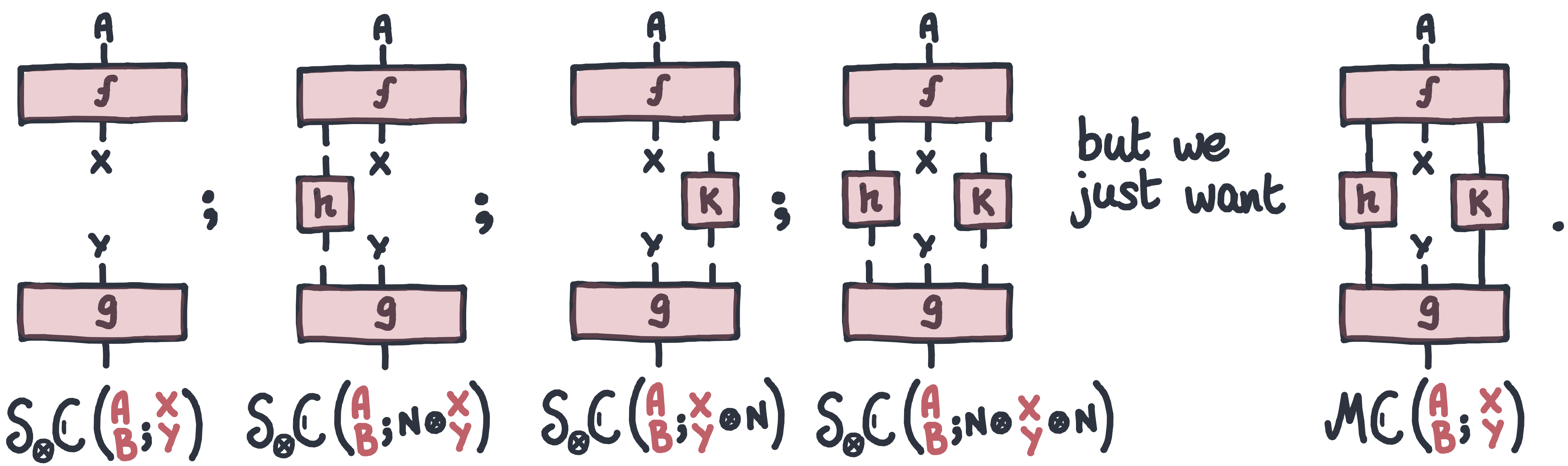


$\begin{bmatrix}X\\Y\end{bmatrix} \triangleleft \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix}$ $\quad N \to \begin{bmatrix}A\\B\end{bmatrix}$ $\quad \begin{bmatrix}X\\Y\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix}$ $\quad \begin{bmatrix}X\\Y\end{bmatrix} \otimes \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix}$ $\quad I \to \begin{bmatrix}A\\B\end{bmatrix}$

Missing

Spliced monoidal arrows have some issues:

- They separate sequential and parallel units unnecessarily.
- Produoidals introduce a lot of bureaucracy on units.



PART 5: NORMALIZATION

OPTICS FOR MONOIDAL CATEGORIES

Normalizing Duoidals

A duoidal $(\triangleleft, N, \otimes, I)$ is normal whenever $I \xrightarrow{\cong} N$.

- Being normal is a property (idempotent monad?).
- However, we cannot normalize any duoidal.

THEOREM (Garner, López Franco). Let $(V, \otimes, I, \triangleleft, N)$ a duoidal with reflexive coequalizers, preserved by $(\otimes)$. Then, $(\mathrm{Bimod}^{\otimes}_{N}, \otimes_N, N, \triangleleft, N)$ is a normal duoidal. Similarly for symmetric duoidals.

Garner & López Franco. Commutativity.

Normalizing Produoidals

Theorem (EHR23). We can ALWAYS normalize a produoidal category. Moreover, $\mathrm{Normalization} \colon \mathrm{Produo} \to \mathrm{Produo}$ is an idempotent monad, constructing a free normalization. Similarly for symmetric produoidals.

Every duoidal is indeed normalizable, but the result may be a produoidal.

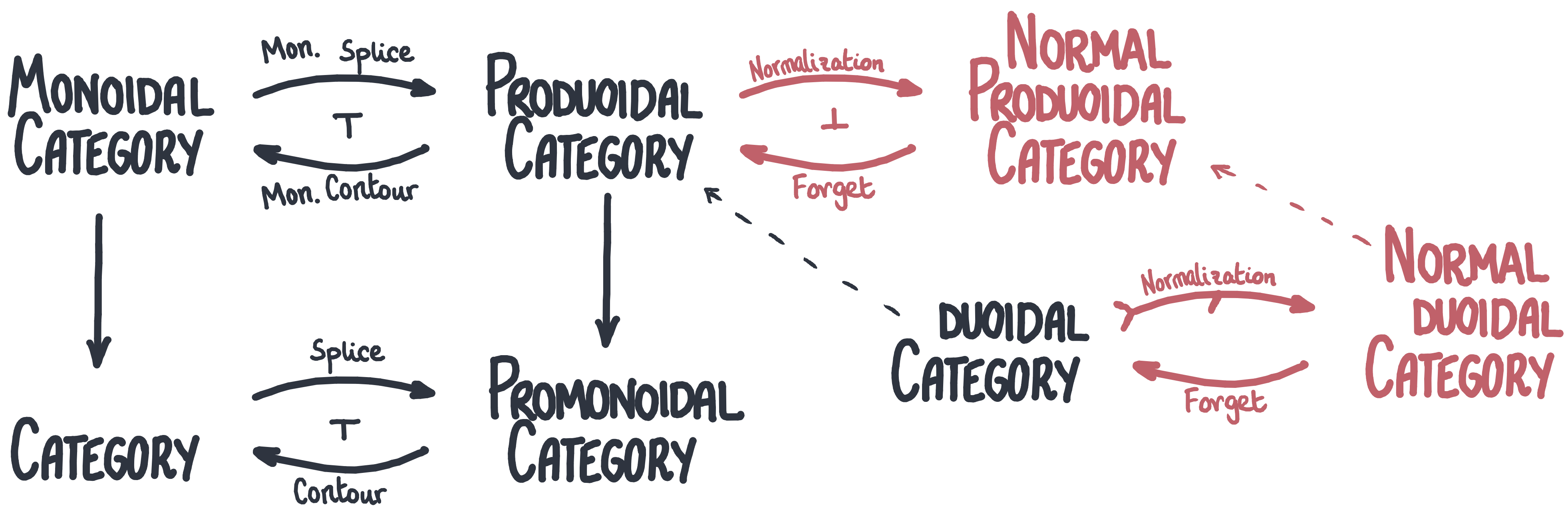
$$\mathcal{N}\mathbb{V}(X;Y) = \mathbb{V}(X; N \otimes Y \otimes N), \qquad \mathcal{N}_{\circ}\mathbb{V}(X;Y) = \mathbb{V}(X; N \otimes Y),$$

$$\mathcal{N}\mathbb{V}(X;Y \triangleleft_N Z) = \mathbb{V}(X;(N \otimes Y \otimes N) \triangleleft (N \otimes Z \otimes N)), \qquad \mathcal{N}_{\circ}\mathbb{V}(X;Y \triangleleft_N Z) = \mathbb{V}(X;(N \otimes Y) \triangleleft (N \otimes Z)),$$

$$\mathcal{N}\mathbb{V}(X;Y \otimes_N Z) = \mathbb{V}(X; N \otimes Y \otimes N \otimes Z \otimes N), \qquad \mathcal{N}_{\circ}\mathbb{V}(X;Y \otimes_N Z) = \mathbb{V}(X; N \otimes Y \otimes Z),$$

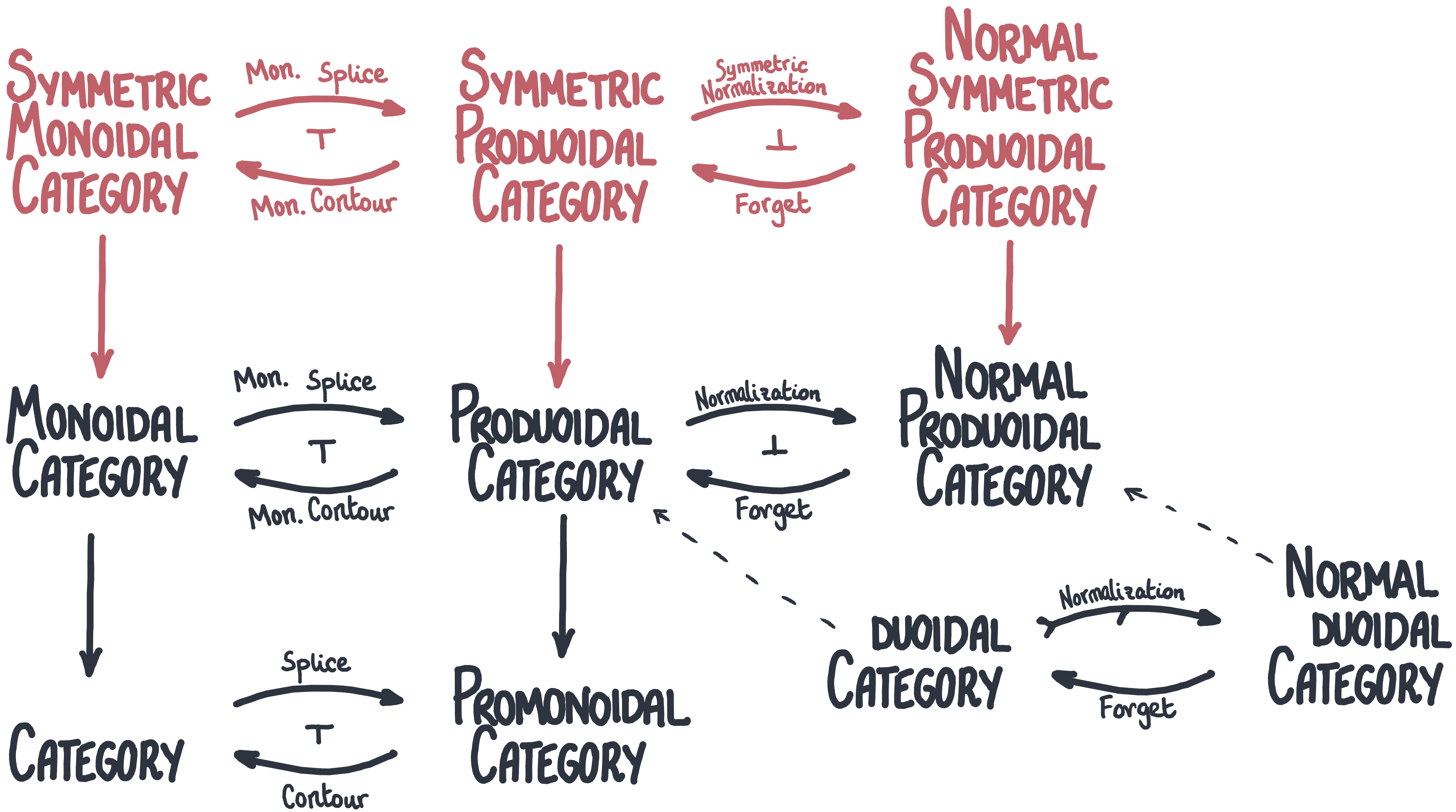
$$\mathcal{N}\mathbb{V}(X;N_N) = \mathcal{N}\mathbb{V}(X;I_N) = \mathbb{V}(X; N), \qquad \mathcal{N}_{\circ}\mathbb{V}(X;N_N) = \mathcal{N}_{\circ}\mathbb{V}(X;I_N) = \mathbb{V}(X; N).$$

Next



Monoidal Category
Mon. Splice
Mon. Contour
Produoidal Category
Normalization
Forget
Normal Produoidal Category
Category
Splice
Contour
Promonoidal Category
Duoidal Category
Normalization
Forget
Normal Duoidal Category

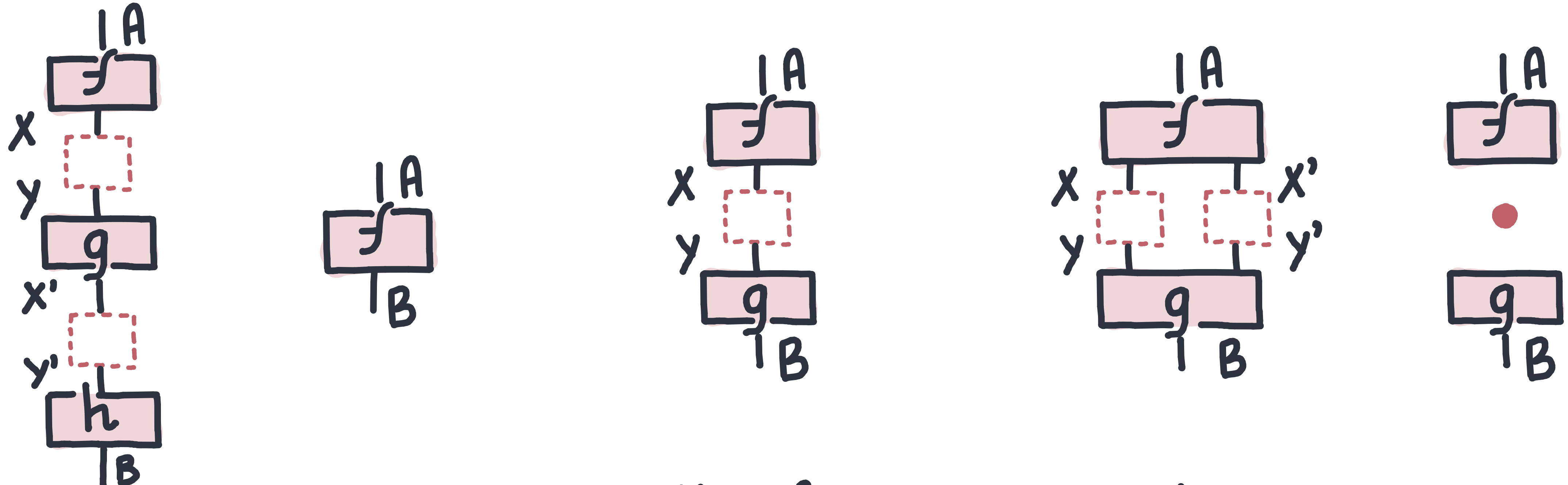
NEXT



Symmetric Monoidal Category
Mon. Splice
⊤
Mon. Contour
Symmetric Produoidal Category
Symmetric Normalization
⊥
Forget
Normal Symmetric Produoidal Category
Monoidal Category
Mon. Splice
⊤
Mon. Contour
Produoidal Category
Normalization
⊥
Forget
Normal Produoidal Category
Category
Splice
⊤
Contour
Promonoidal Category
Duoidal Category
Normalization
Forget
Normal Duoidal Category

Monoidal Context

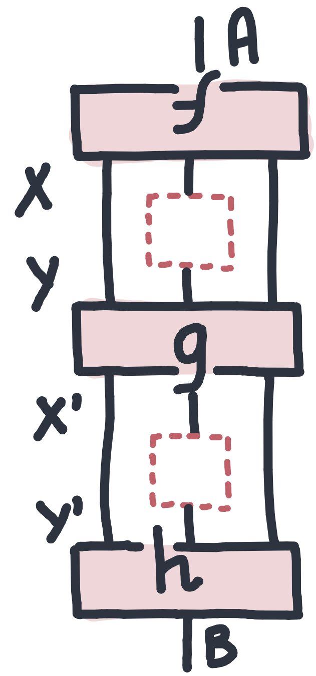
THM (EHR'23). Monoidal context is the cofree produoidal on a monoidal.



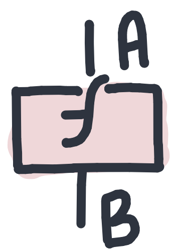
$\begin{bmatrix}X\\Y\end{bmatrix} \triangleleft \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix}$ $\quad N \to \begin{bmatrix}A\\B\end{bmatrix}$ $\quad \begin{bmatrix}X\\Y\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix}$ $\quad \begin{bmatrix}X\\Y\end{bmatrix} \otimes \begin{bmatrix}X'\\Y'\end{bmatrix} \to \begin{bmatrix}A\\B\end{bmatrix}$ $\quad I \to \begin{bmatrix}A\\B\end{bmatrix}$

Normalized Monoidal Context

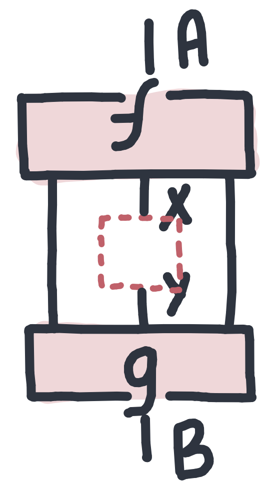
THM (EHR'23). Monoidal optics are the free normalization of monoidal context.



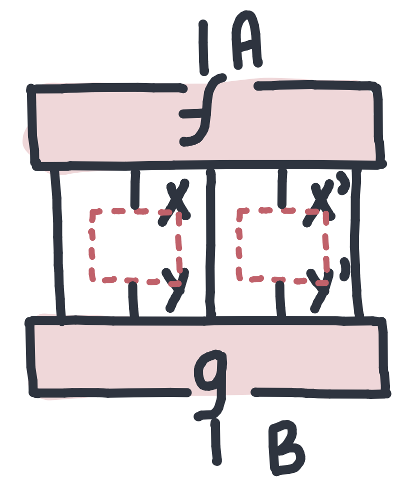
$$\begin{bmatrix} X \\ Y \end{bmatrix} \triangleleft \begin{bmatrix} X' \\ Y' \end{bmatrix} \to \begin{bmatrix} A \\ B \end{bmatrix}$$



$$\begin{bmatrix} A \\ B \end{bmatrix}$$



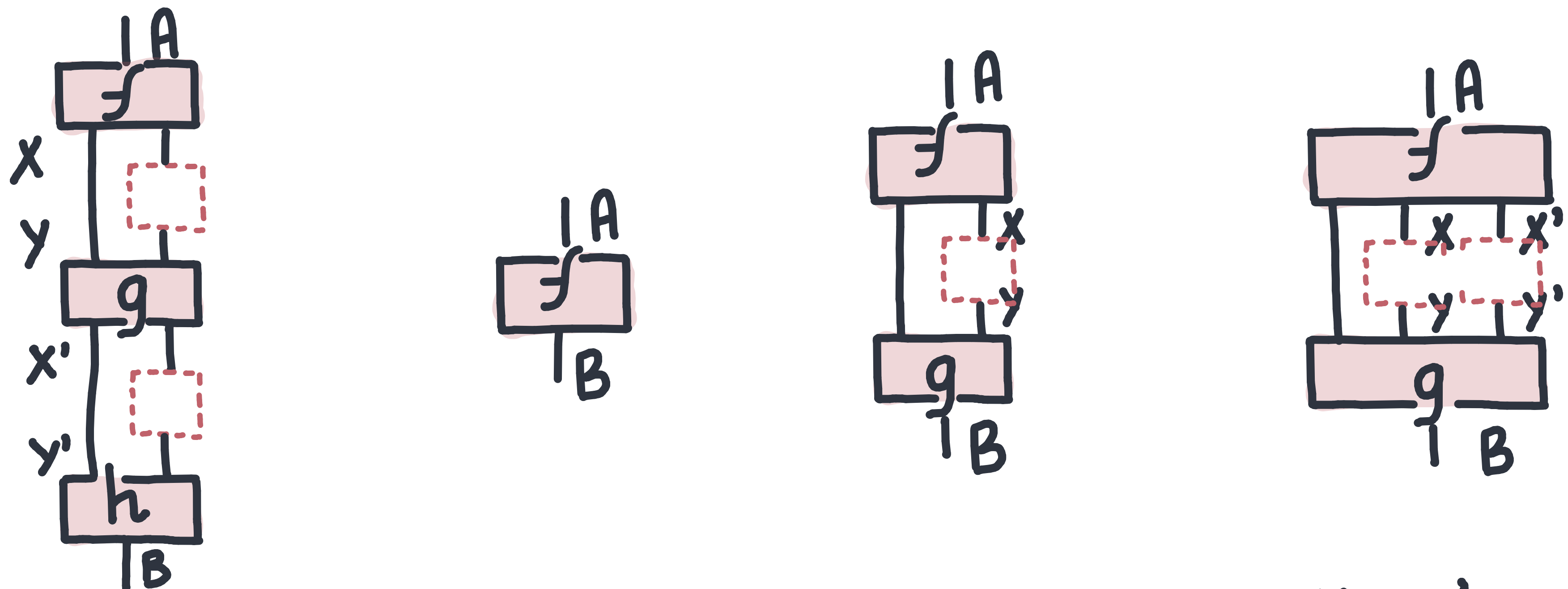
$$\begin{bmatrix} X \\ Y \end{bmatrix} \to \begin{bmatrix} A \\ B \end{bmatrix}$$



$$\begin{bmatrix} X \\ Y \end{bmatrix} \otimes \begin{bmatrix} X' \\ Y' \end{bmatrix} \to \begin{bmatrix} A \\ B \end{bmatrix}$$

Normalized Symmetric Monoidal Context

Thm (EHR'23). Monoidal optics are the free normalization of monoidal context.

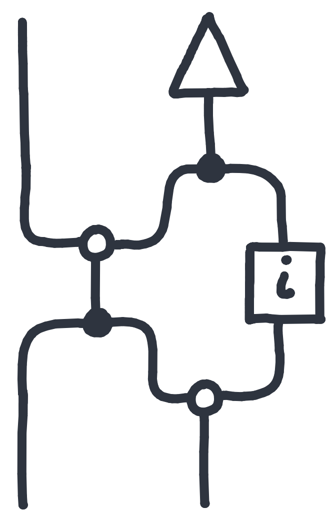


$\begin{bmatrix} X \\ Y \end{bmatrix} \triangleleft \begin{bmatrix} X' \\ Y' \end{bmatrix} \to \begin{bmatrix} A \\ B \end{bmatrix}$ $\quad \begin{bmatrix} A \\ B \end{bmatrix}$ $\quad \begin{bmatrix} X \\ Y \end{bmatrix} \to \begin{bmatrix} A \\ B \end{bmatrix}$ $\quad \begin{bmatrix} X \\ Y \end{bmatrix} \otimes \begin{bmatrix} X' \\ Y' \end{bmatrix} \to \begin{bmatrix} A \\ B \end{bmatrix}$

Part 6: Example

ONE-TIME PAD

Broadbent & Karvonen propose a formalization of the one-time pad in a monoidal category with a Hopf algebra with an integral.

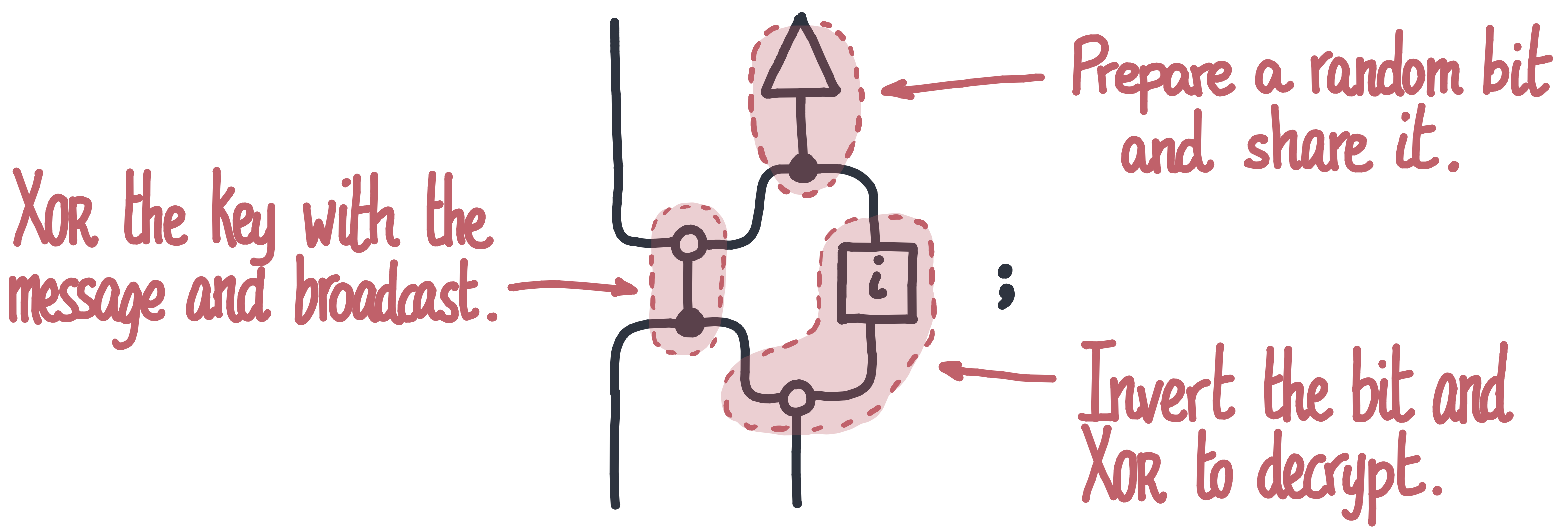


;

Broadbent & Karvonen. Categorical Composable Cryptography.

ONE-TIME PAD

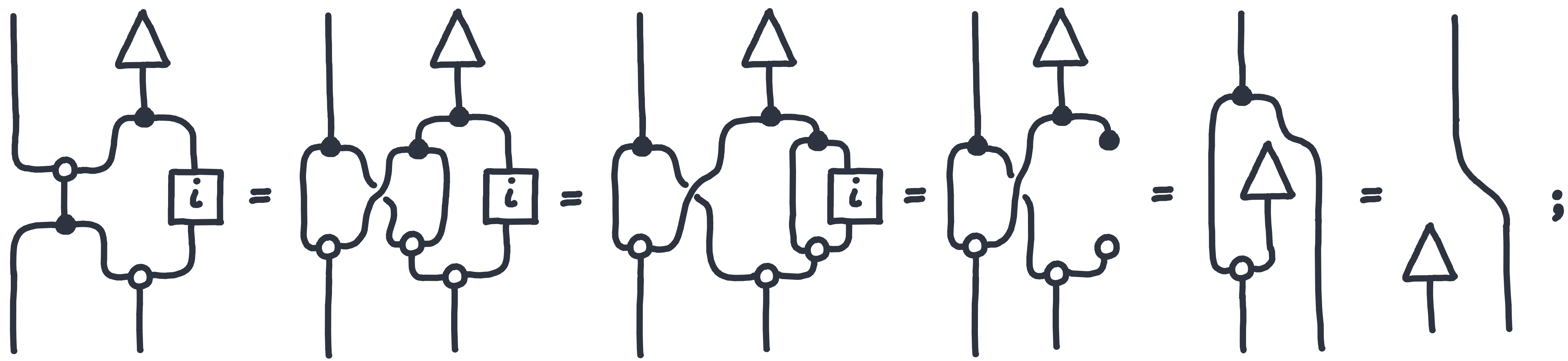
Broadbent & Karvonen propose a formalization of the one-time pad in a monoidal category with a Hopf algebra with an integral.



Broadbent & Karvonen. Categorical Composable Cryptography.

One-Time Pad

Broadbent & Karvonen propose a formalization of the one-time pad in a monoidal category with a Hopf algebra with an integral.

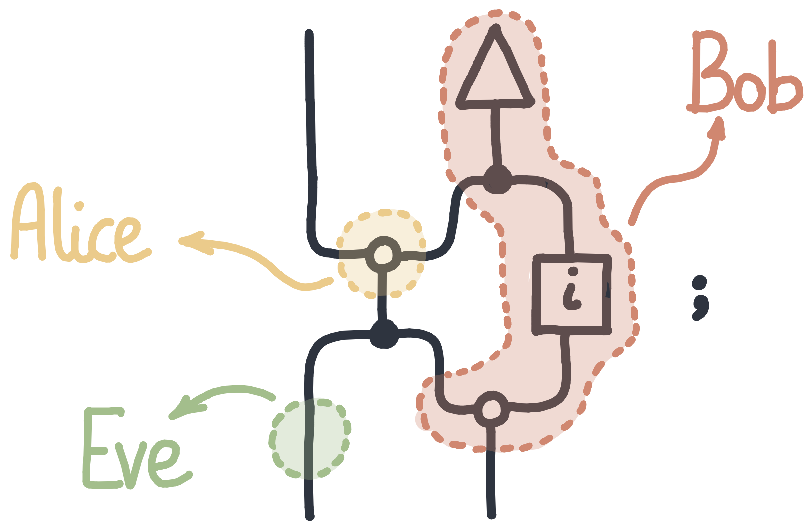


We can reason about security using string diagrams.

Broadbent & Karvonen. Categorical Composable Cryptography.

ONE-TIME PAD

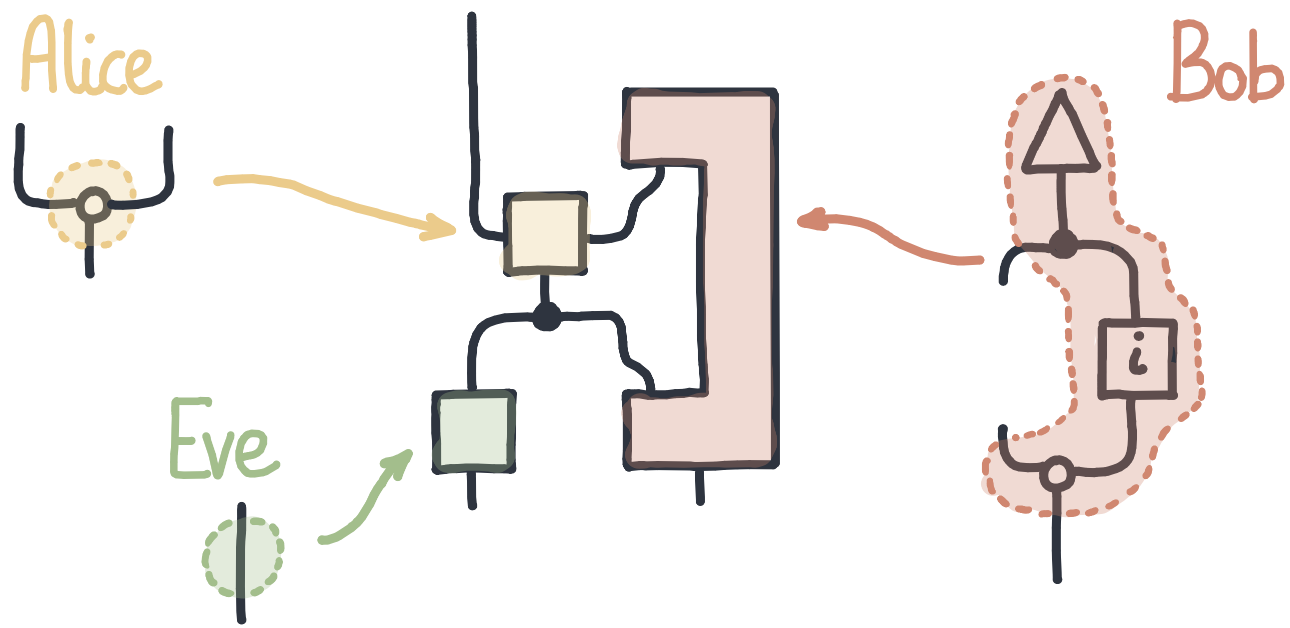
We want to split the morphism into different agents: Alice does not control the broadcast; Eve can only attack at the end; Bob keeps a bit in memory.



;

ONE-TIME PAD

We want to split the morphism into different agents: Alice does not control the broadcast; Eve can only attack at the end; Bob keeps a bit in memory.



The set of possible actions of Alice and Eve are given by a hom-set; they are monoidal morphisms. What about Bob?

One-Time Pad

This is not only about string diagrams; this is about code modularity and separation.

```
oneTimePad(msg) = do
  key <- randomBit
  crypt <- xor(msg,key)
  msg <- xor(crypt,key)
  return msg
```

Do-notation is a syntax for (pre)monoidal categories; following string diagrams. We can extend it with message-passing, and split into components.

Heunen & Jacobs, Hughes, Staton & Levy, Román.

ONE-TIME PAD

github.com/mroman42/one-time-pad-example

This is not only about string diagrams; this is about code modularity and separation.

```
oneTimePad(alice,bob,eve,msg) = do
  key <- bob₀()
  crypt <- alice(msg, key)
  () <- eve(crypt)
  msg <- bob₁(crypt)
  return msg
```

```
alice(msg, key) = do
  crypt <- xor(msg,key)
  return crypt
```

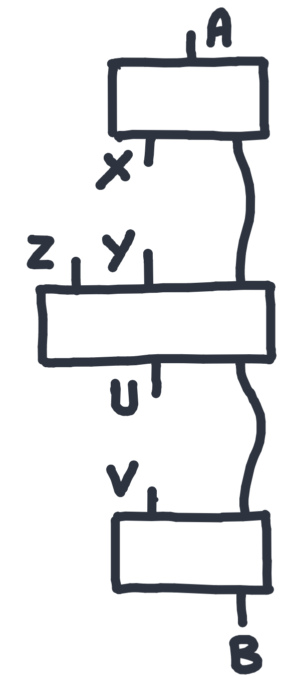
```
eve(crypt) = do
  return crypt
```

```
bob() = do
  key <- randomBit
  !key
  ?crypt
  msg <- xor(crypt,key)
  return msg
```

FURTHER WORK

In the category of lenses, we can write exchanges, e.g.

$$\mathcal{LC}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; \left(\begin{smallmatrix}X\\Y\end{smallmatrix} \otimes \begin{smallmatrix}I\\Z\end{smallmatrix}\right) \triangleleft \begin{smallmatrix}U\\V\end{smallmatrix}\right)$$



PROPOSITION. The $\otimes$ of lenses is representable. Lenses are monoidal with $\binom{X}{Y} \otimes \binom{X'}{Y'} = \binom{X \otimes X'}{Y \otimes Y'}$.

$$\mathcal{LC}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; \begin{smallmatrix}X\\Y\otimes Z\end{smallmatrix} \triangleleft \begin{smallmatrix}U\\V\end{smallmatrix}\right)$$

PROPOSITION. There exist mon. functors $(!) \colon \mathcal{C} \to \mathcal{LC}$ and $(?) \colon \mathcal{C}^{op} \to \mathcal{LC}$. These satisfy $!X = \binom{X}{I}$, $?X = \binom{I}{X}$, with $\binom{X}{Y} = !X \otimes ?Y = !X \triangleleft ?Y$,

! SEND

? RECEIVE

$$\mathcal{LC}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; !X \triangleleft ?(Y \otimes Z) \triangleleft !U \triangleleft ?V\right).$$

Honda et al.

END