Monoidal Context

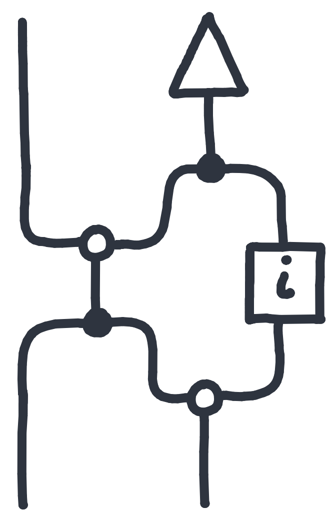
Mario Román joint with Matt Earnshaw and James Hefford

Ottawa Logic Seminar, 1st March

Supported by the EU Estonian IT Academy.

ONE-TIME PAD

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

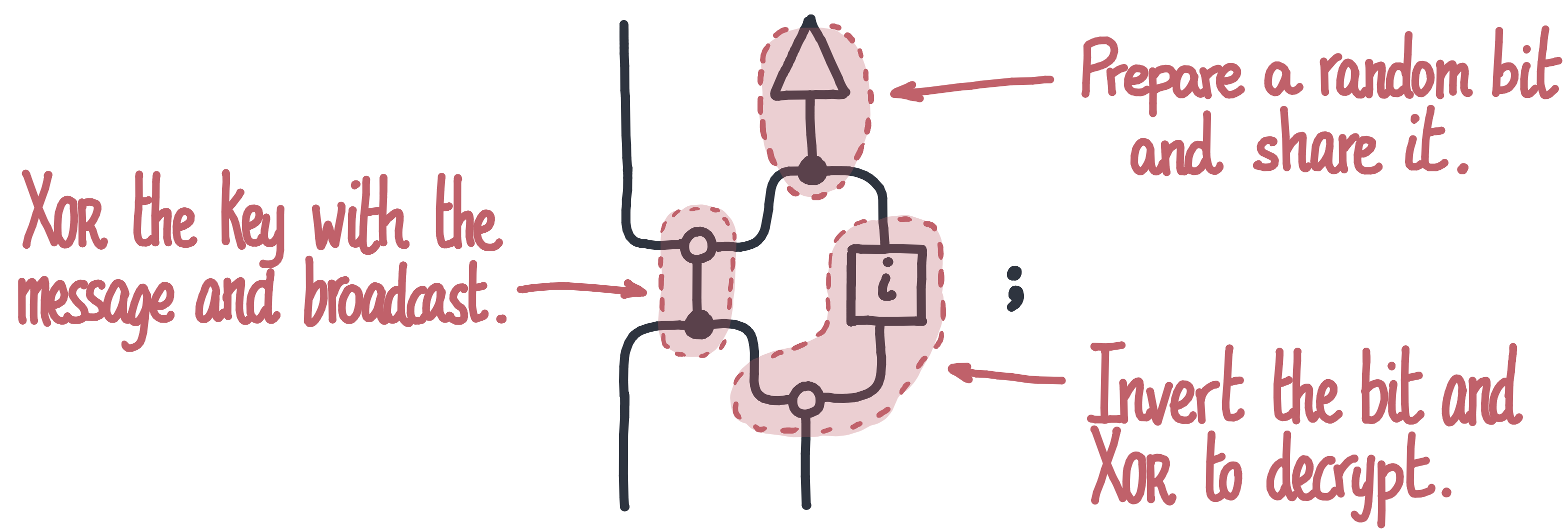


;

Broadbent & Karvonen. Categorical Composable Cryptography.

ONE-TIME PAD

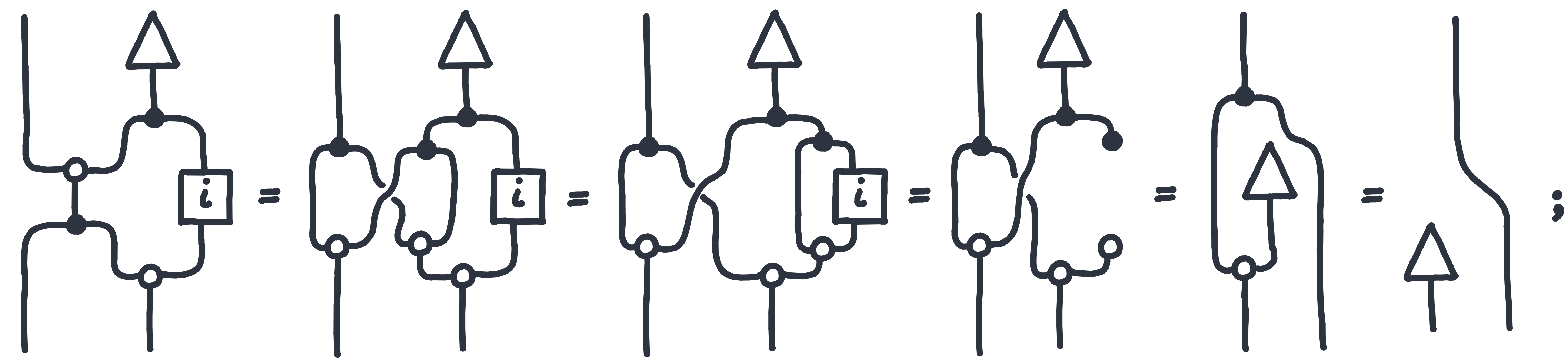
Broadbent & Karvonen propose a formalization of the one-time pad in a monoidal category with a Hopf algebra with an integral.



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.

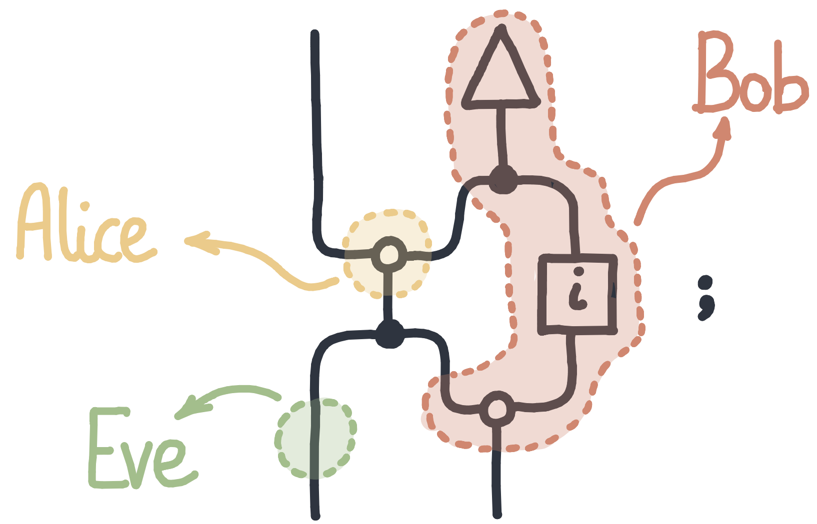


We can reason about security using string diagrams.

Broadbent & Karvonen. Categorical Composable Cryptography.

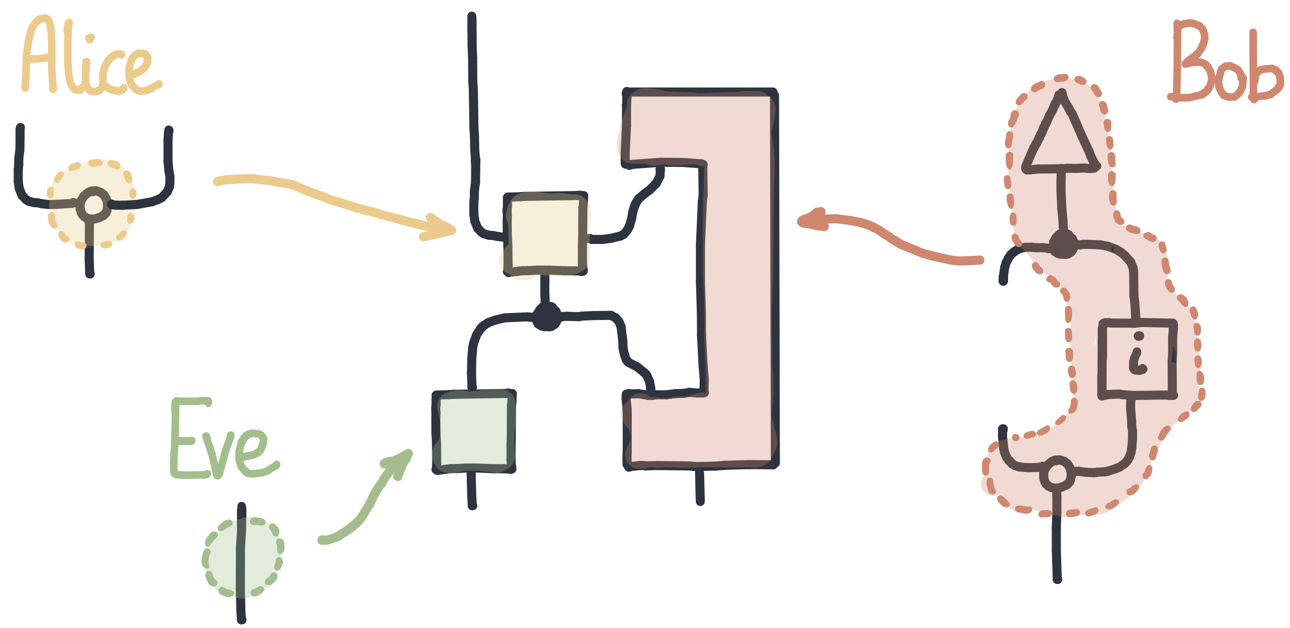
ONE-TIME PAD

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.

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

ONE-TIME PAD

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

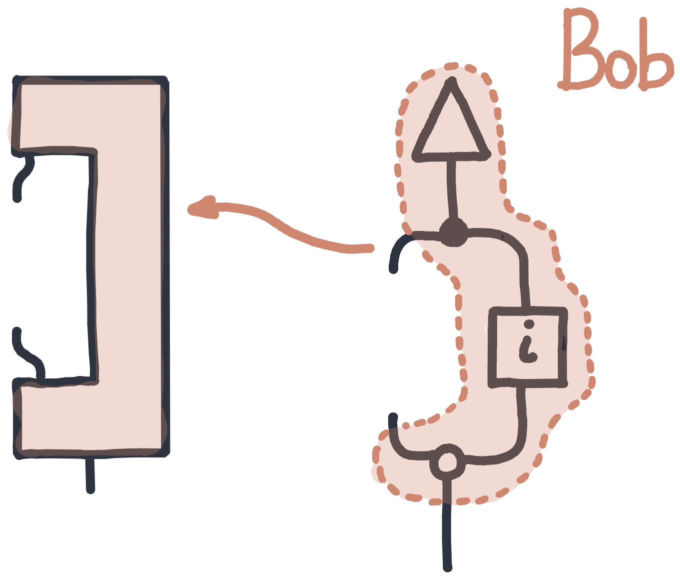
```
oneTimePad(alice,bob,eve,msg) = do
  key <- bob₀()
  crypt <- alice(msg, key)
  () <- eve(crypt)
  msg <- bob₁(crypt)
  return msg
```

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

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

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

SUMMARY



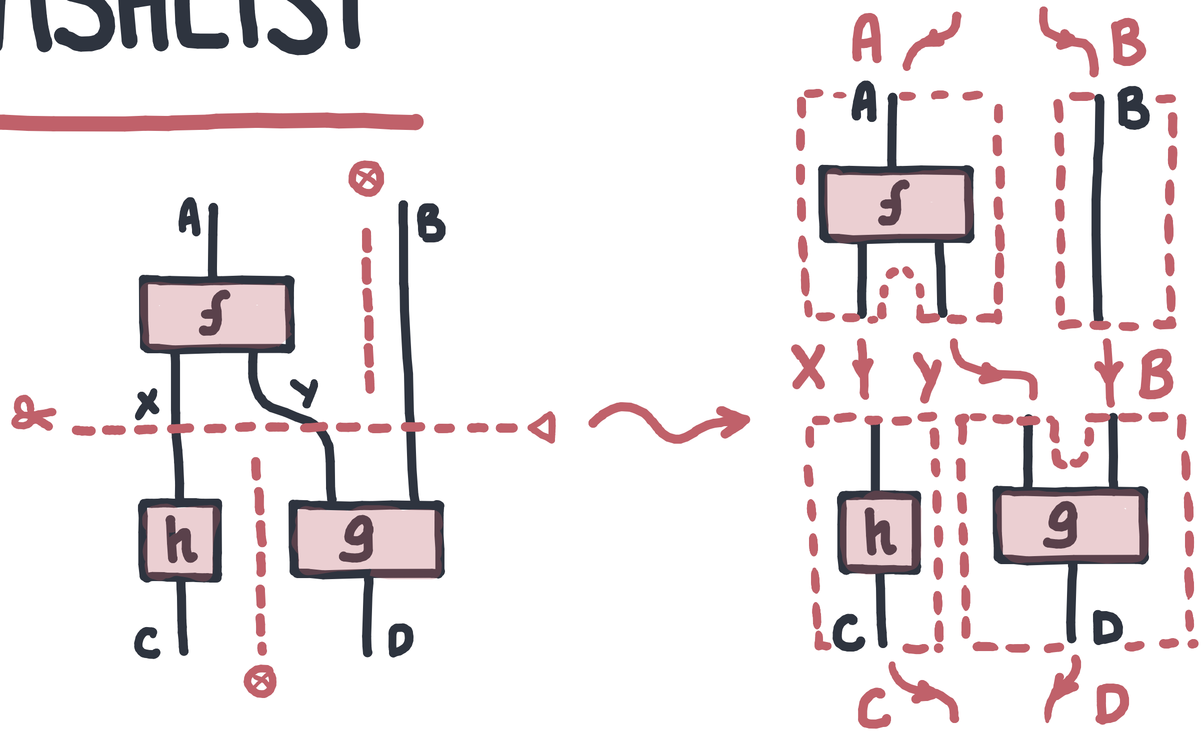
What are these incomplete diagrams?

M.R. Open Diagrams via Coend Calculus.

Which structure do they form?

Matt Earnshaw, James Hefford, M.R.
The Produoidal Algebra of Process Decomposition.

WISHLIST



$A \otimes B$ splits into
$(A\otimes B) \triangleleft ((X \otimes Y)\otimes B) \triangleleft (X \otimes (Y \otimes B)) \triangleleft (C \otimes D)$
to get to $C \otimes D$

Algebra of parallel/sequential decomposition. (Pro)duoidal categories.

Semantics of incomplete diagrams. Monoidal context.

Message-passing. Send-Receive types.

Summary

- Part 1. Profunctors
- Part 2. Promonoidal Categories
- Part 3. Context for Categories
- Part 4. Context for Monoidal Categories
- Part 5. Normal Context for Monoidal Categories
- Part 6. Normal Context for Symmetric Monoidal Categories
- Part 7. Send/Receive Session Types

Part 1 : Profunctors, Dinaturality

PROFUNCTORS (FUNCTORS $\mathbb{C}^{op} \times \mathbb{D} \to \mathbf{SET}$)

Profunctors are sets of processes $\mathbf{P}(X;Y)$ indexed contravariantly by a inputs $X \in \mathbb{C}^{op}$ and covariantly by outputs. $Y \in \mathbb{D}$. They have actions.

$$(>) : \mathbb{C}(X';X) \times \mathbf{P}(X;Y) \to \mathbf{P}(X';Y),$$
$$(<) : \mathbf{P}(X;Y) \times \mathbb{D}(Y;Y') \to \mathbf{P}(X;Y'),$$

satisfying

$f > (p < g) = (f > p) < g\ ;$		compatibility
$f_0 > f_1 > p = (f_0 ⨾ f_1) > p\ ;$	$id > p = p\ ;$	left action
$p < g_0 < g_1 = p < (g_0 ⨾ g_1)\ ;$	$p < id = p.$	right action

Profunctor Composition

A process of the composite type $P;Q$ is a process in P communicating with one in Q. That is, $\langle p | q \rangle \in P;Q\,(X,Z)$ is given by $p \in P(X,Y)$ followed by $q \in Q(Y,Z)$ for some Y.

Given $p \in P(X;Y_0)$, $q \in Q(Y_1;Z)$, and a morphism $f \in \mathbb{B}(Y_0;Y_1)$, we can

- execute p to get a Y_0, then execute q with f,
- execute p with f to get a Y_1, then execute q.

$$\langle p < f \mid q \rangle \sim_d \langle p \mid f > q \rangle.$$

These are "dinaturally" equivalent.

Coends are the colimits that arise by quotienting by dinatural equivalence.

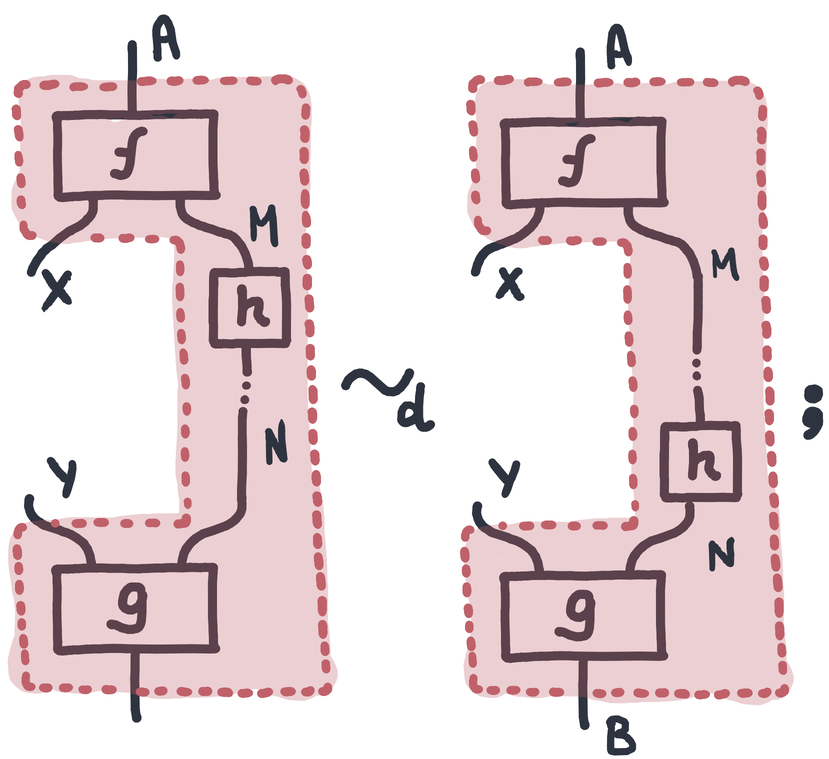
$$\int^{Y \in \mathbb{B}} P(X;Y) \times Q(Y;Z)$$

$$:=$$

$$\coprod_{Y \in \mathbb{B}} P(X;Y) \times Q(Y;Z) \Big/ {\sim_d} \,.$$

Dinaturality

We could define contexts as pairs of morphisms, but we would like the following two to be equal.



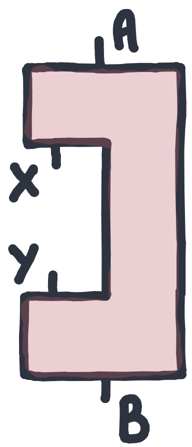
DEFINITION. A context of type $(A;B)$ with a hole $(X;Y)$ is a pair of morphisms $\langle f, g\rangle_M$ with
$f : A \to M \otimes X$ and $g : M \otimes Y \to B$,
quotiented by dinaturality.

$$\langle f \mathbin{;} (h \otimes id) \mid g \rangle \sim_d \langle f \mid (h \otimes id) \mathbin{;} g \rangle.$$

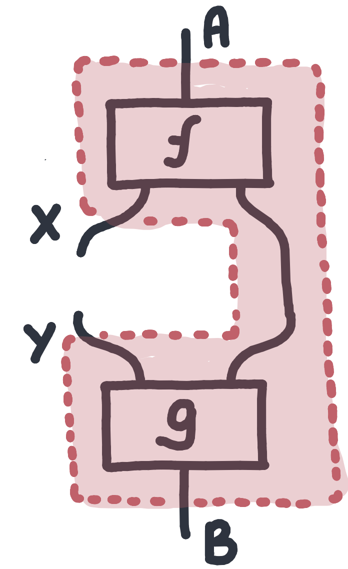
In other words, it is an element of

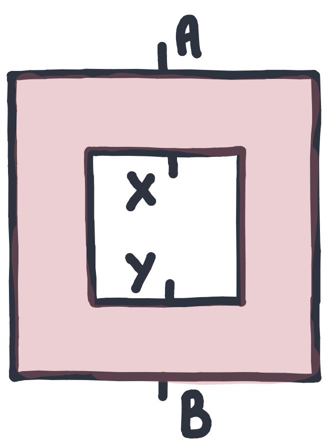
$$\int^{M \in \mathbb{C}} \mathbb{C}(A; X \otimes M) \times \mathbb{C}(Y \otimes M; B).$$

Open Diagrams

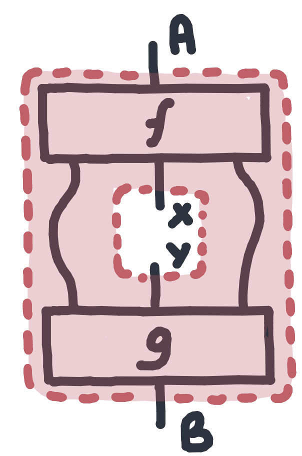


$$\rightsquigarrow \int^{M} \hom(A; X \otimes M) \times \hom(Y \otimes M; B) \rightsquigarrow$$

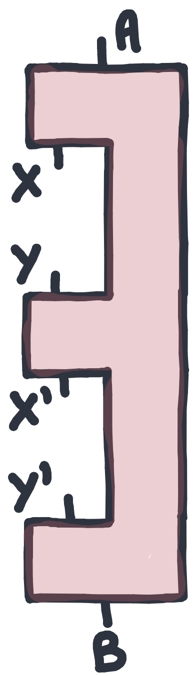




$$\rightsquigarrow \int^{M} \hom(A; M \otimes X \otimes N) \times \hom(M \otimes Y \otimes N; B) \rightsquigarrow$$

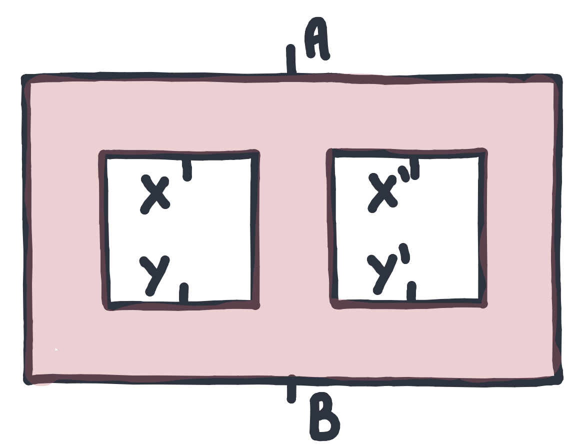


Open Diagrams

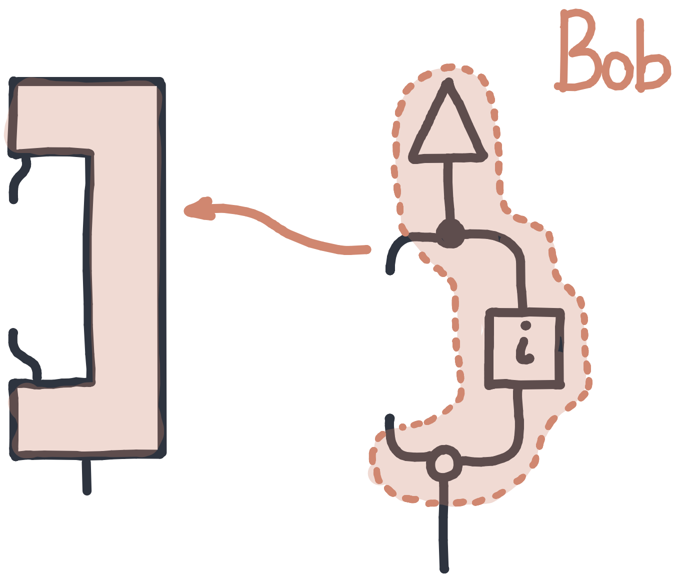


$$\int^{M} \hom(A; X \otimes M) \times \hom(Y \otimes M; X' \otimes N) \times \hom(Y' \otimes N; B)$$

$$\int^{M,N,O} \hom(A; M \otimes X \otimes N \otimes X' \otimes O) \times \hom(M \otimes Y \otimes N \otimes Y' \otimes O; B)$$



SUMMARY



What are these incomplete diagrams?

M.R. Open Diagrams via Coend Calculus.

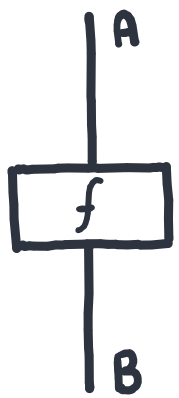
Which structure do they form?

Matt Earnshaw, James Hefford, M.R.
The Produoidal Algebra of Process Decomposition.

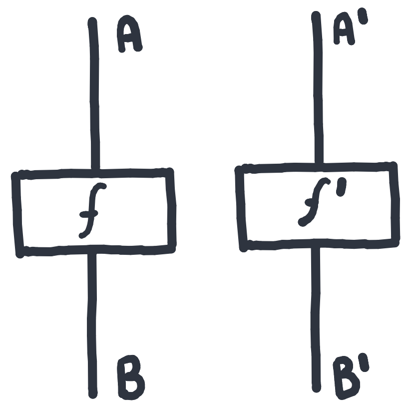
Part 2: Promonoidals

Monoidal Categories: Process Theories

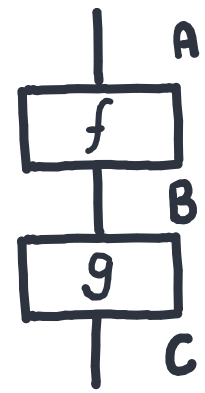
Monoidal categories are an algebra of parallel and sequential composition.
String diagrams are the internal language of monoidal categories.



Process



Parallel composition



Sequential composition

Bènabou

MONOIDAL CATEGORY

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

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

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

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

and natural bijections,

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

satisfying the pentagon and triangle equations.

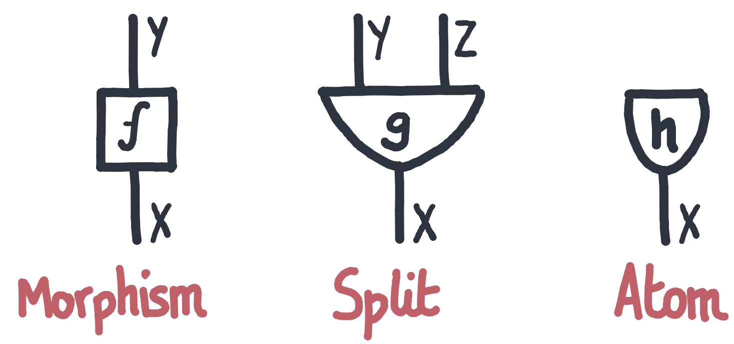
By nesting, $\mathbb{C}(\bullet;X\otimes(Y\otimes Z))$, we mean profunctor composition,

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

PROMONOIDAL CATEGORIES

Promonoidal categories provide a theory of coherent decomposition. It has

- Morphisms, $\mathbb{C}(X;Y)$.
- Splits, $\mathbb{C}(X;Y \otimes Z)$.
- Atoms, $\mathbb{C}(X;I)$.

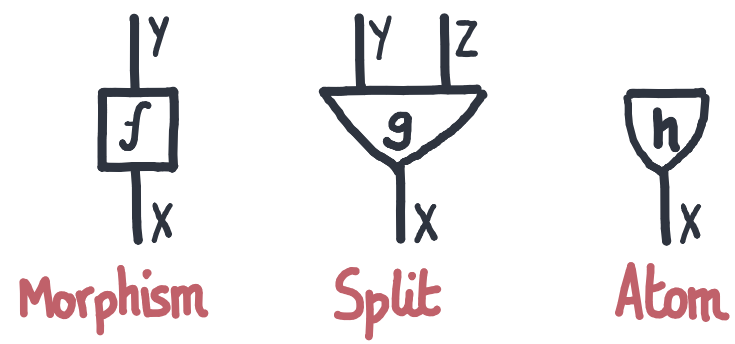


Coherence property: i.e. splitting A into X and "something" and then splitting that something into Y and Z can be done in the same number of ways as splitting A into "something" and Z and then splitting that something into X and Y.

ProMonoidal Categories

Promonoidal categories provide a theory of coherent decomposition. It has

- Morphisms, $\mathbb{C}(X;Y)$.
- Splits, $\mathbb{C}(X;Y \otimes Z)$.
- Atoms, $\mathbb{C}(X;I)$.

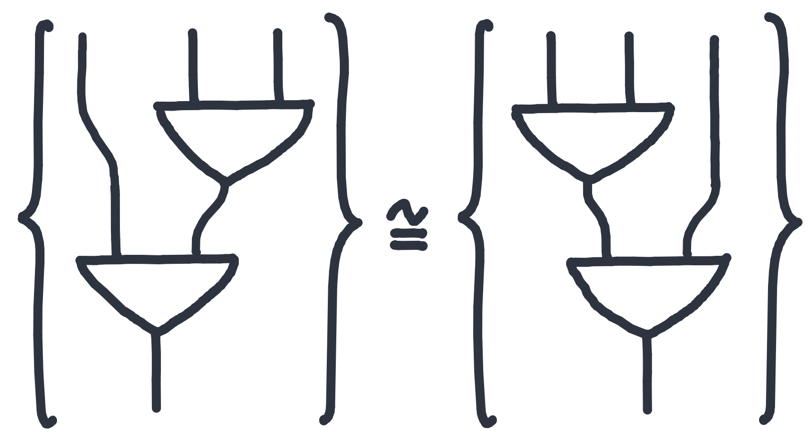


Coherence property:

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

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

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



Part 3 : Context for Categories

Splice-Contour

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

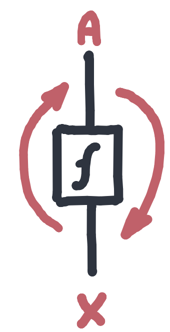
- Each promonoidal gives a free category. Contour
- Each category gives a cofree promonoidal. Splice

$$\begin{tikzcd} \mathrm{Cat} \arrow[rr, bend right, "\mathrm{Splice}"'] \arrow[rr, phantom, "\perp"] & & \mathrm{PromonCat} \arrow[ll, bend right, "\mathrm{Contour}"'] \end{tikzcd}$$

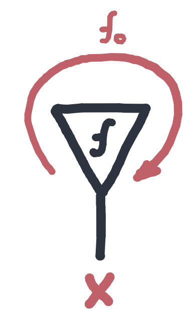
Melliès & Zeilberger. Parsing as a Lifting Problem.

Contour

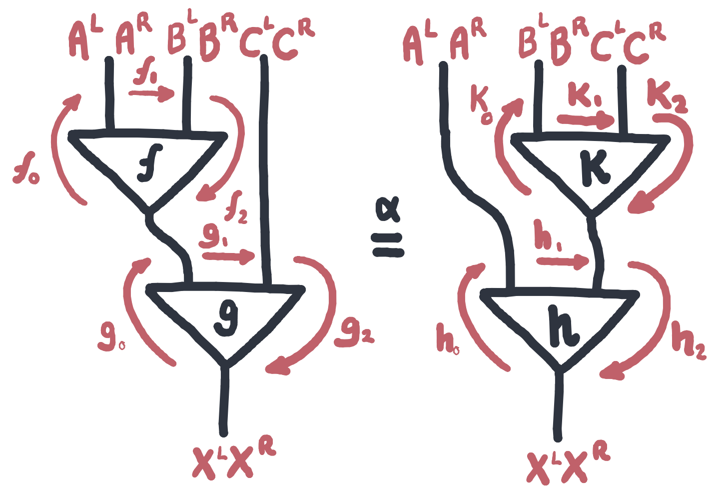
$f_0 : X^L \to A^L$
$f_1 : A^R \to B^L$
$f_2 : B^R \to X^R$



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



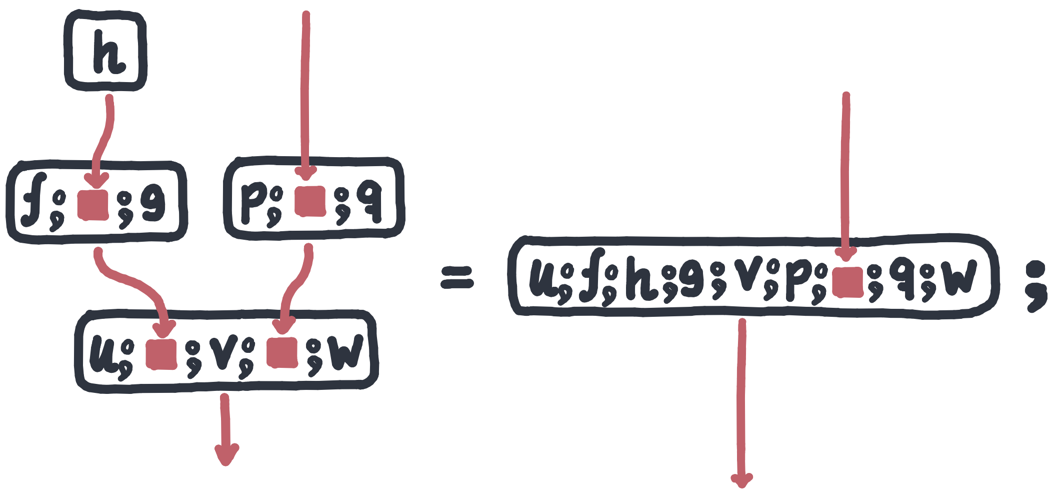
$f_0 : X^L \to X^R$



Contouring a promonoidal gives a category that follows decomposition,

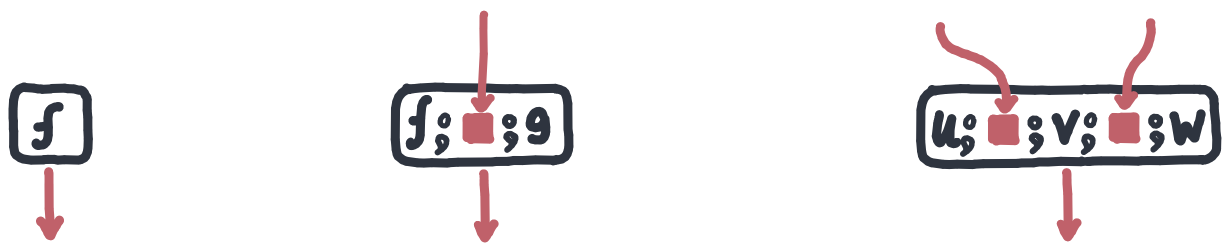
$$\textsc{Promon} \longrightarrow \textsc{Cat}.$$

Splice



Splice is right adjoint to contour.

$\mathbf{Cat} \longrightarrow \mathbf{Promon}.$



$S\begin{pmatrix}A\\B\end{pmatrix}$ $\quad S\begin{pmatrix}A & X\\B & Y\end{pmatrix}$ $\quad S\begin{pmatrix}A & X & X'\\B & Y & Y'\end{pmatrix}$

Splice-Contour

We can rewrite Melliès & Zeilberger for promonoidals instead of multicategories.

- Universal context: cofree promonoidal.
- Morphisms with holes: $u ⨾ \blacksquare ⨾ v ⨾ \blacksquare ⨾ w$.
- $\mathrm{Splice}(\mathbb{C})$ is the monoid of the duality $\mathbb{C} \dashv \mathbb{C}^{op}$.
- Can we do the same for monoidal categories?

Melliès & Zeilberger. Parsing as a Lifting Problem.

Part 4 : Context for Monoidal Categories

WHAT NEXT

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

Duoidals

An extra dimension side-steps Eckmann-Hilton.

Definition. A duoidal category is a category $\mathbb{V}$ with two promonoidal structures

$\triangleleft : \mathbb{V} \times \mathbb{V} \to \mathbb{V}$, "seq. split" $\qquad N : 1 \to \mathbb{V}$, "seq unit"

$\otimes : \mathbb{V} \times \mathbb{V} \to \mathbb{V}$, "par. split" $\qquad I : 1 \to \mathbb{V}$, "par. unit"

such that one laxly distributes over the other,

$$\psi_2 : (A \triangleleft B) \otimes (C \triangleleft D) \longrightarrow (A \otimes C) \triangleleft (B \otimes D),$$
$$\psi_0 : I \longrightarrow N,$$
$$\varphi_2 : N \longrightarrow N \triangleleft N,$$
$$\varphi_0 : I \longrightarrow I \otimes I.$$

We ask coherence for these maps.

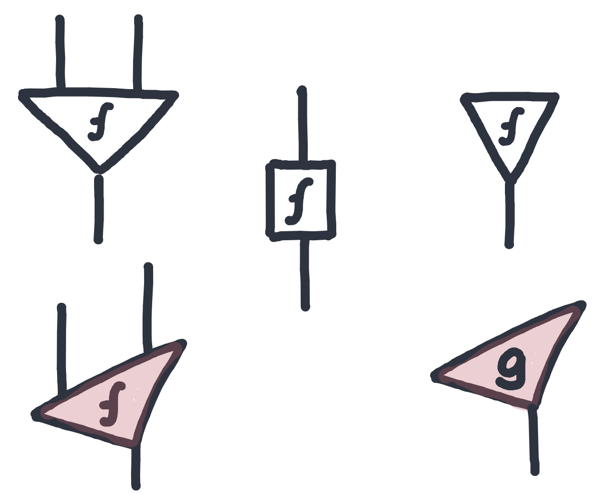
Produoidal Categories

Definition. A *produoidal category* is a category $\mathbb{V}$ with two promonoidal structures

$$\mathbb{V}(\bullet;\bullet\triangleleft\bullet)\colon \mathbb{V}^{op}\times\mathbb{V}\times\mathbb{V}\to \mathrm{Set}, \text{ "seq. split"} \qquad \mathbb{V}(\bullet;N)\colon \mathbb{V}^{op}\to \mathrm{Set}, \text{ "seq. unit"}$$
$$\mathbb{V}(\bullet;\bullet\otimes\bullet)\colon \mathbb{V}^{op}\times\mathbb{V}\times\mathbb{V}\to \mathrm{Set}, \text{ "par. split"} \qquad \mathbb{V}(\bullet;I)\colon \mathbb{V}^{op}\to \mathrm{Set}, \text{ "par. unit"}$$

such that one laxly distributes over the other,

$$\psi_2\colon \mathbb{V}(X;(A\triangleleft B)\otimes(C\triangleleft D)) \longrightarrow \mathbb{V}(X;(A\otimes C)\triangleleft(B\otimes D)),$$
$$\psi_0\colon \mathbb{V}(X;I) \longrightarrow \mathbb{V}(X;N),$$
$$\varphi_2\colon \mathbb{V}(X;N) \longrightarrow \mathbb{V}(X;N\triangleleft N),$$
$$\varphi_0\colon \mathbb{V}(X;I) \longrightarrow \mathbb{V}(X;I\otimes I).$$



We ask coherence for these maps.

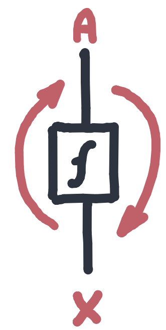
Monoidal Splice-Contour

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

- Each produoidal gives a free monoidal category. Contour
- Each monoidal category gives a cofree produoidal. Splice

$$
\begin{tikzcd}
\mathsf{MonCat} \arrow[rr, bend right, "\text{Mon.Splice}"'] \arrow[rr, phantom, "\perp"] & & \mathsf{ProduoCat} \arrow[ll, bend right, "\text{Mon.Contour}"']
\end{tikzcd}
$$

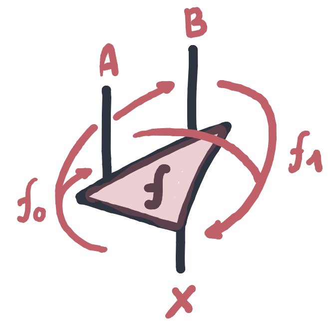
MONOIDAL SPLICE-CONTOUR



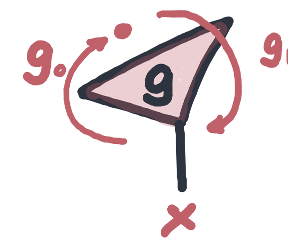
$f_0 : X^L \to A^L$
$f_1 : A^R \to X^R$

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

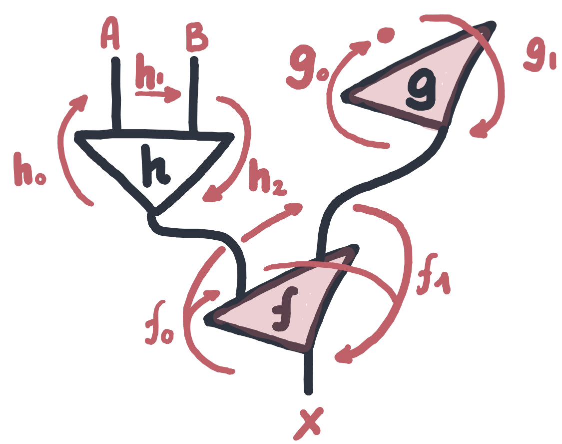
$f_0 : X^L \to A^L$
$f_1 : A^R \to B^L$
$f_2 : B^R \to X^R$



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

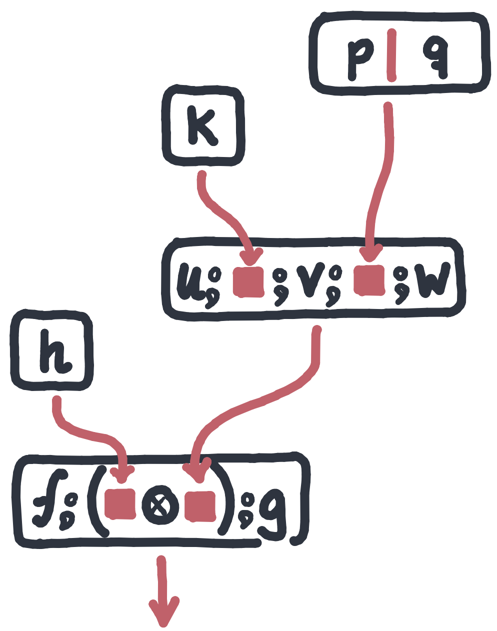


$g_0 : X^L \to I$
$g_1 : I \to X^R$

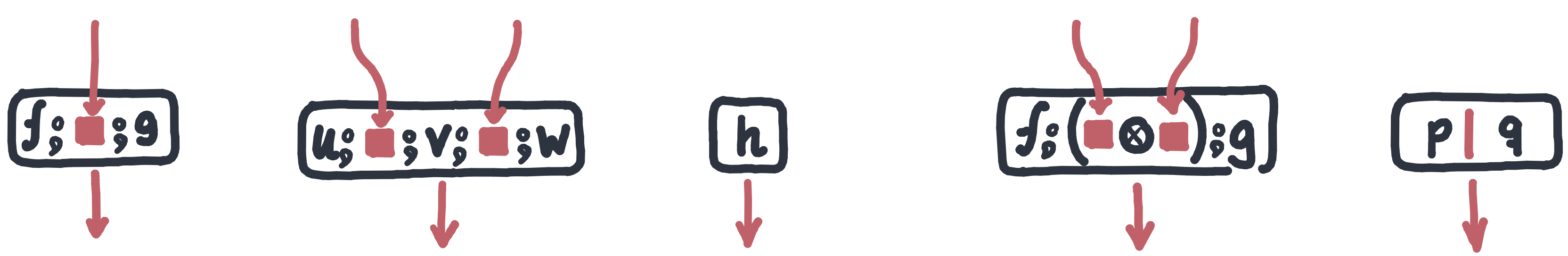


Contouring a produoidal gives a mon. category that tracks decomposition.

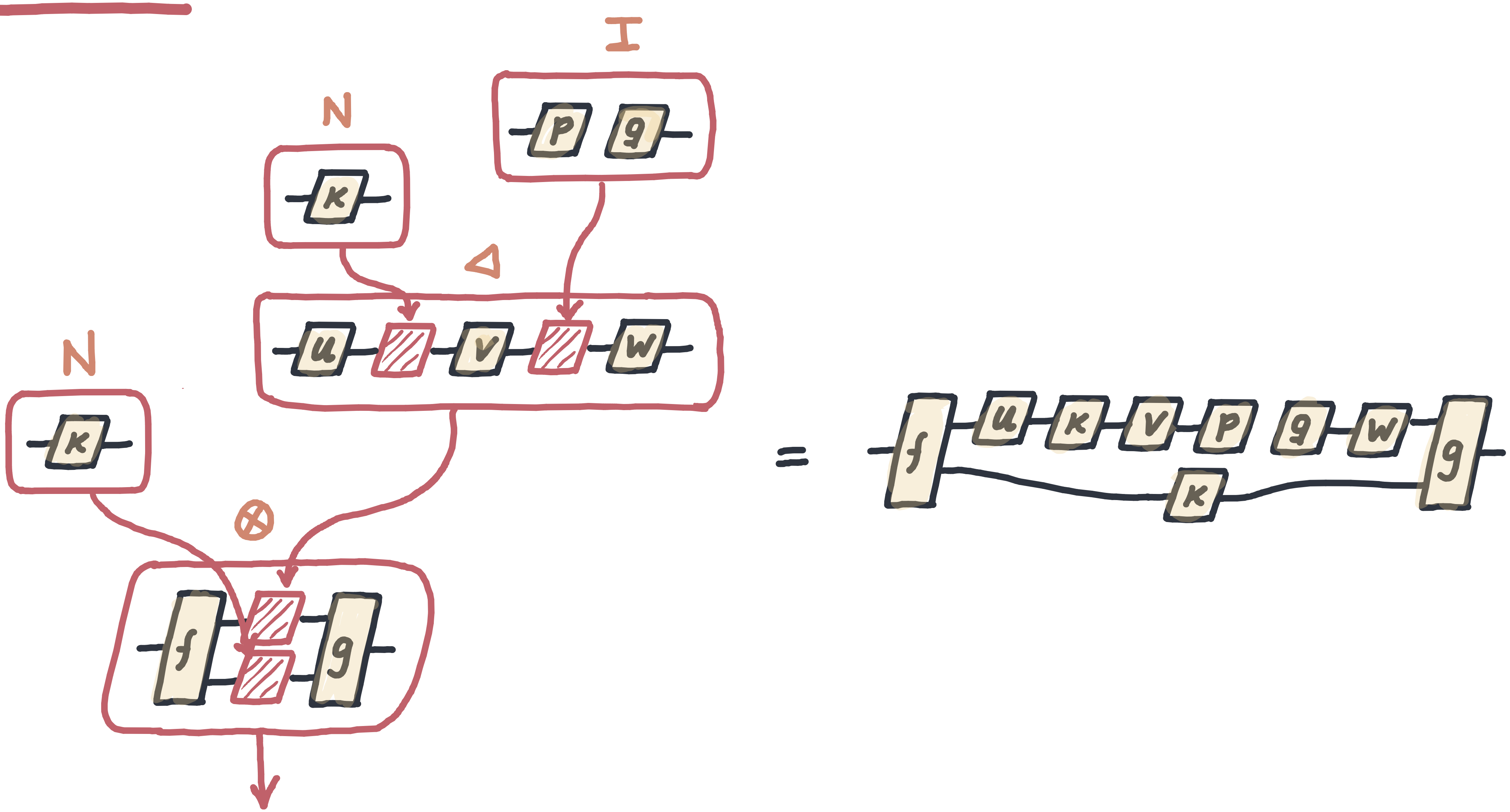
Monoidal Splice-Contour



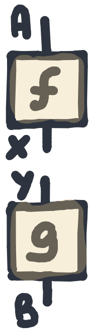
$$= f \mathbin{;} (h \otimes (u \mathbin{;} k \mathbin{;} v \mathbin{;} p \mathbin{;} q \mathbin{;} w)) \mathbin{;} g$$



Monoidal Splice-Contour



Spliced Monoidal Arrows

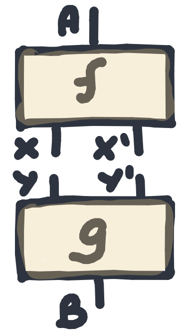


$S_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; \begin{smallmatrix}X\\Y\end{smallmatrix}\right)$

morphism

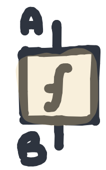
$S_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; \begin{smallmatrix}X\\Y\end{smallmatrix} \triangleleft \begin{smallmatrix}X'\\Y'\end{smallmatrix}\right)$

sequential split



$S_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; \begin{smallmatrix}X\\Y\end{smallmatrix} \otimes \begin{smallmatrix}X'\\Y'\end{smallmatrix}\right)$

parallel split



$S_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; N\right)$

sequential unit

$S_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; I\right)$

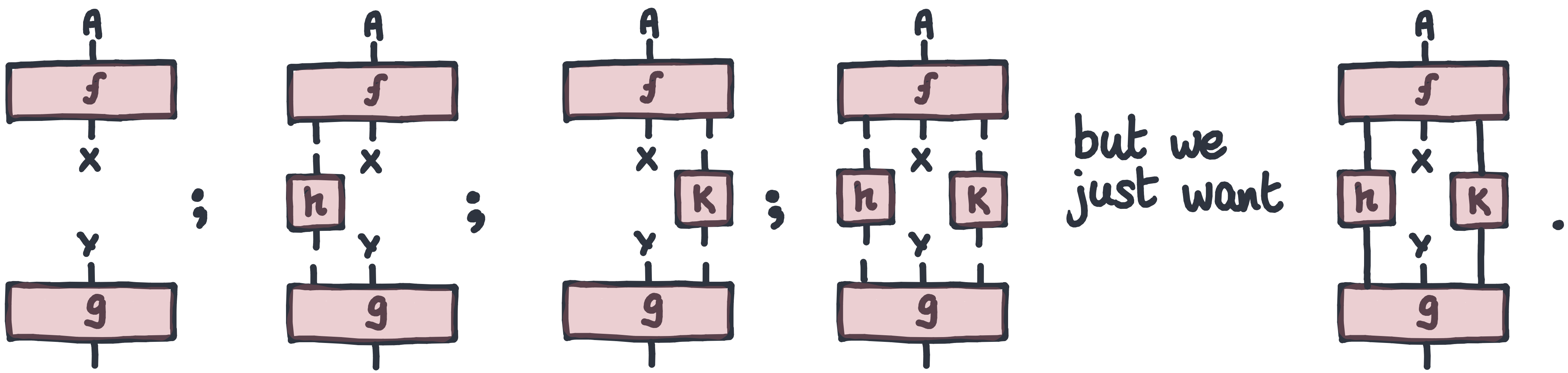
parallel unit

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

Missing

Spliced monoidal arrows have some issues:

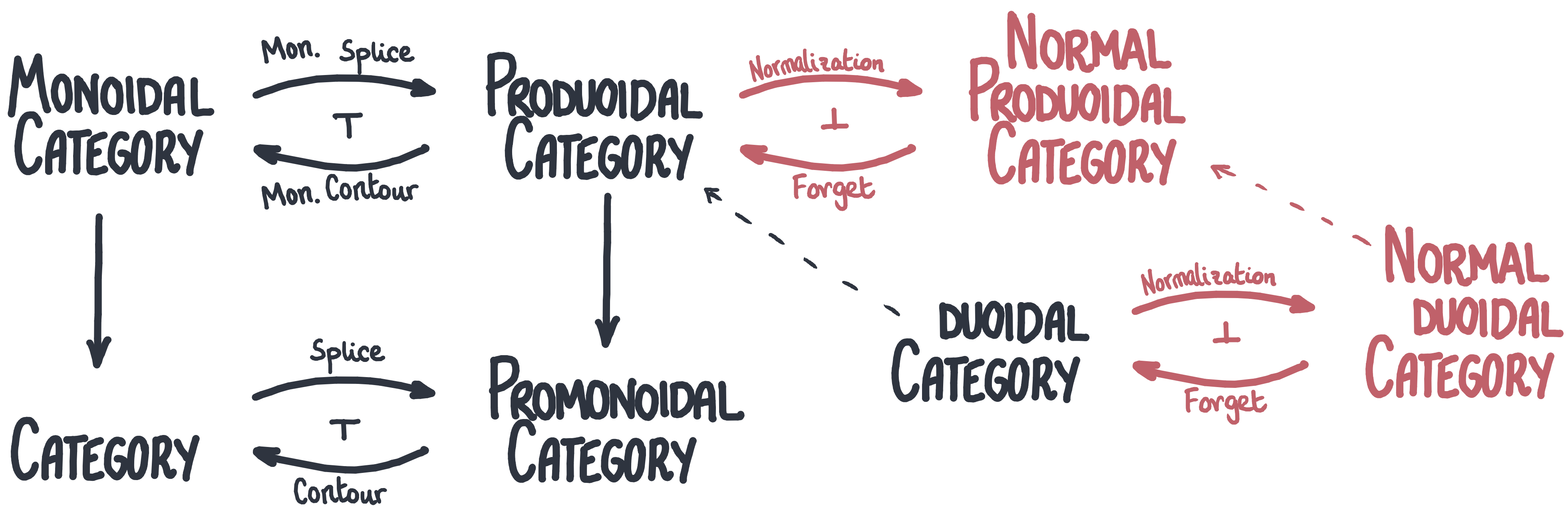
- They separate sequential and parallel units unnecessarily.
- Produoidals introduce a lot of bureaucracy on units.



$\mathcal{S}_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; \begin{smallmatrix}X\\Y\end{smallmatrix}\right)$ $\mathcal{S}_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; N \otimes \begin{smallmatrix}X\\Y\end{smallmatrix}\right)$ $\mathcal{S}_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; \begin{smallmatrix}X\\Y\end{smallmatrix} \otimes N\right)$ $\mathcal{S}_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; N \otimes \begin{smallmatrix}X\\Y\end{smallmatrix} \otimes N\right)$ $\mathcal{M}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; \begin{smallmatrix}X\\Y\end{smallmatrix}\right)$

Part 5: Normal Context for Monoidal Categories

WHAT 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

Normalizing Duoidals

A duoidal $(\triangleleft, N, \otimes, I)$ is **normal** whenever $I \to N$ is an iso.

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

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

Garner & López Franco. Commutativity.

Normalizing Produoidals

We can ALWAYS[(!)] normalize a produoidal category $(\mathbb{V}, \otimes, I, \triangleleft, N)$.
Every duoidal is indeed normalizable, but the result may be a produoidal.

THEOREM (EHR23). Let $(\mathbb{V}, \otimes, I, \triangleleft, N)$ a produoidal category. Then, $(\mathcal{N}_\sigma\mathbb{V}, \otimes_N, \triangleleft_N, N)$ is a normal produoidal. Moreover, $\mathcal{N} : \mathrm{Produo} \to \mathrm{Produo}$ is an idempotent monad.

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

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

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

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

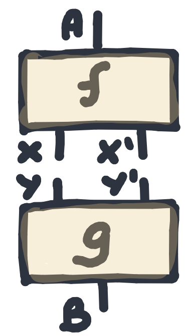
Recap: Spliced Monoidal Arrows

$S_\otimes\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};\begin{smallmatrix}X\\Y\end{smallmatrix}\right)$

morphism

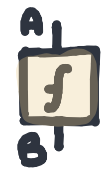
$S_\otimes\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};\begin{smallmatrix}X\\Y\end{smallmatrix}\triangleleft\begin{smallmatrix}X'\\Y'\end{smallmatrix}\right)$

sequential split



$S_\otimes\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};\begin{smallmatrix}X\\Y\end{smallmatrix}\otimes\begin{smallmatrix}X'\\Y'\end{smallmatrix}\right)$

parallel split



$S_\otimes\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};N\right)$

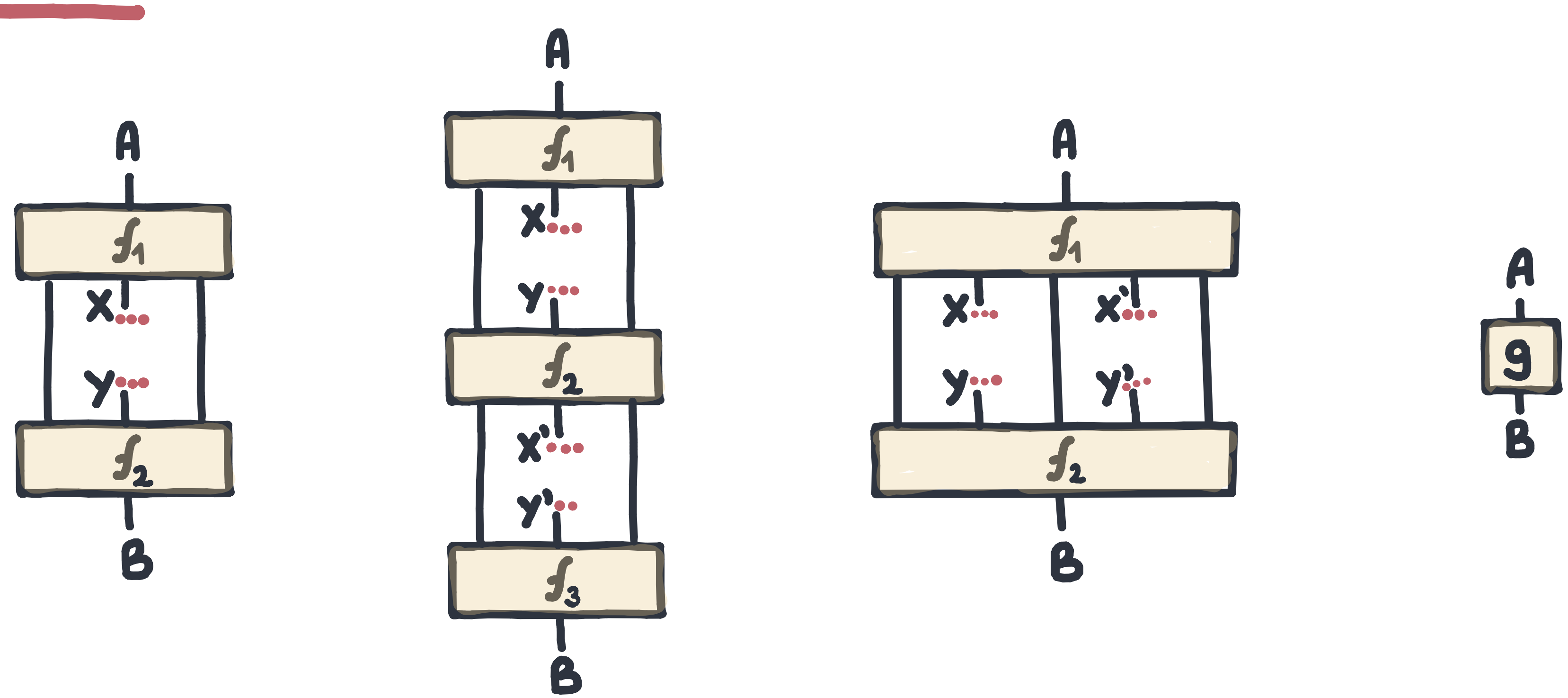
sequential unit

$S_\otimes\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};I\right)$

parallel unit

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

Monoidal Context



$\mathbb{MC}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; \begin{smallmatrix}X\\Y\end{smallmatrix}\right)$
morphism

$\mathbb{MC}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; \begin{smallmatrix}X\\Y\end{smallmatrix} \triangleleft \begin{smallmatrix}X'\\Y'\end{smallmatrix}\right)$
sequential split

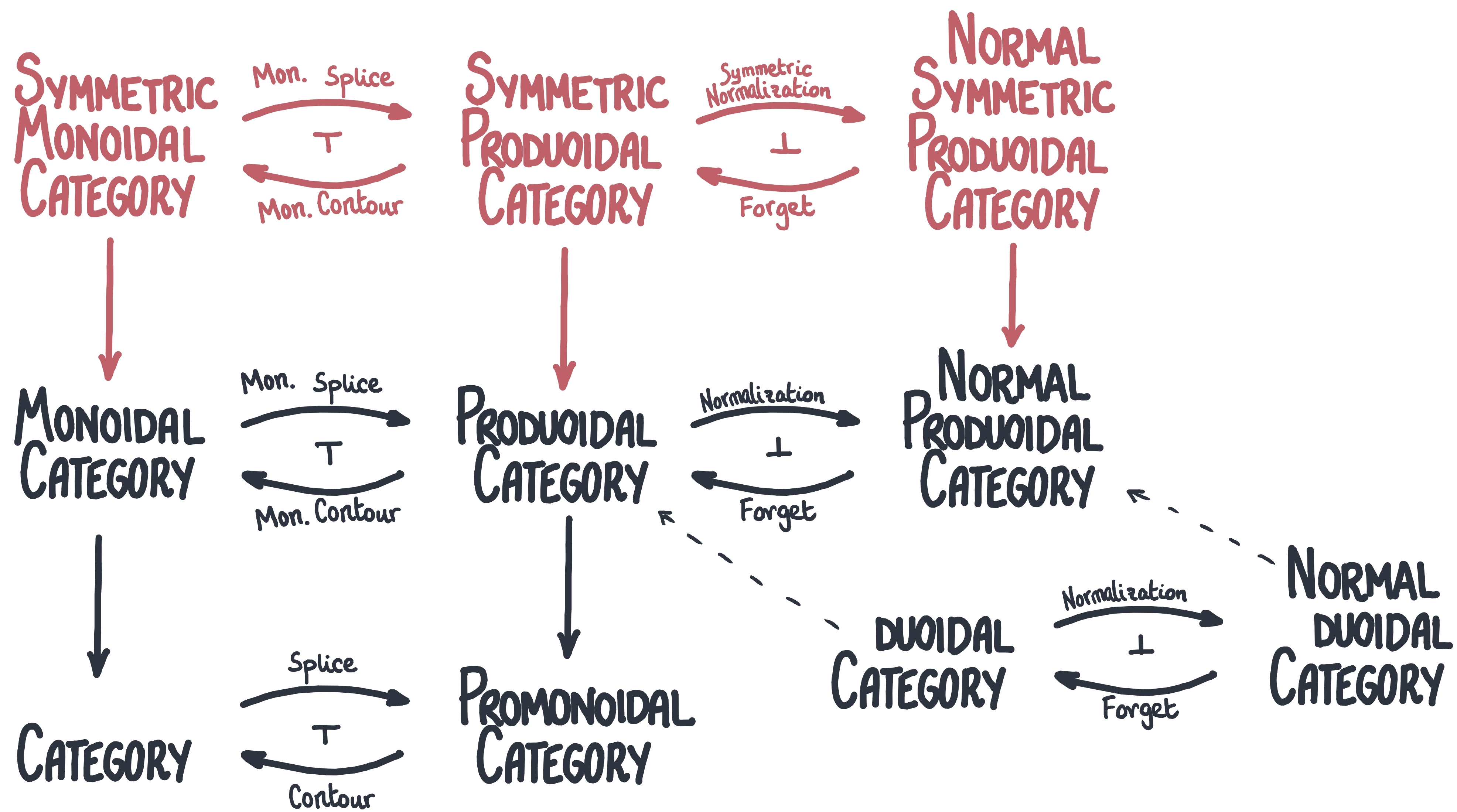
$\mathbb{MC}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; \begin{smallmatrix}X\\Y\end{smallmatrix} \otimes \begin{smallmatrix}X'\\Y'\end{smallmatrix}\right)$
parallel split

$\mathbb{MC}\left(\begin{smallmatrix}A\\B\end{smallmatrix}; N\right)$
unit

THM (EHR'23). Monoidal context is the free normalization of spliced monoidal arrows.

Part 6 : Normal Context for Symm. Monoidal Categories

What 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

Normalizing Symmetric Duoidals

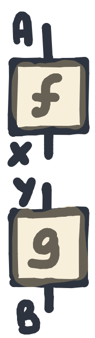
A duoidal $(\triangleleft, N, \otimes, I)$ is $\otimes$-symmetric whenever $\otimes, I$ is symm. monoidal.

- We can normalize symmetric duoidals as usual.
- However, there is a more specialized procedure.

THEOREM (Garner, López Franco). Let $(V, \otimes, I, \triangleleft, N)$ a sym.$^{\otimes}$ duoidal with reflexive coequalizers, preserved by $(\otimes)$. Then, $(\mathrm{Mod}^{\otimes}_{N}, \otimes_{N}, N, \triangleleft, N)$ is a normal sym.$^{\otimes}$ duoidal.

Garner & López Franco. Commutativity.

Recap: Spliced Monoidal Arrows

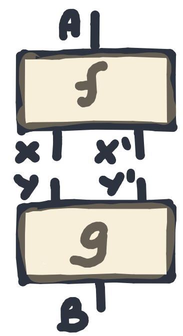


$S_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};\begin{smallmatrix}X\\Y\end{smallmatrix}\right)$

morphism

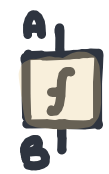
$S_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};\begin{smallmatrix}X\\Y\end{smallmatrix}\triangleleft\begin{smallmatrix}X'\\Y'\end{smallmatrix}\right)$

sequential split



$S_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};\begin{smallmatrix}X\\Y\end{smallmatrix}\otimes\begin{smallmatrix}X'\\Y'\end{smallmatrix}\right)$

parallel split



$S_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};N\right)$

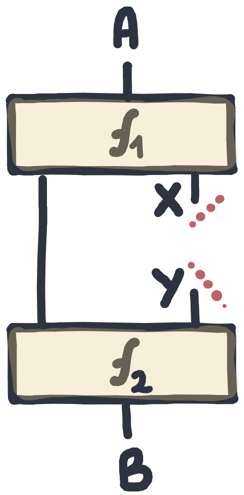
sequential unit

$S_{\otimes}\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};I\right)$

parallel unit

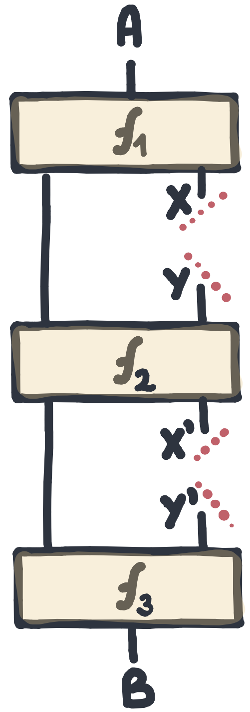
THM (EHR'23). Spliced monoidal arrows are the cofree produoidal on a monoidal.

Monoidal Lenses



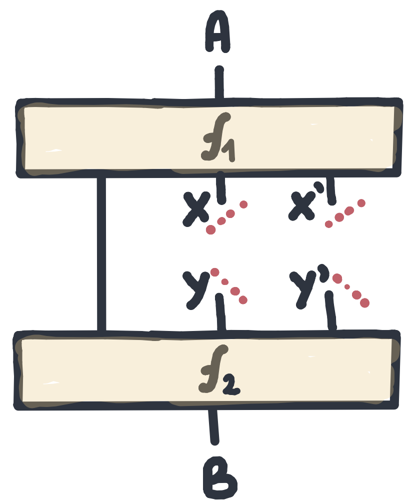
$L\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};\begin{smallmatrix}X\\Y\end{smallmatrix}\right)$

morphism



$L\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};\begin{smallmatrix}X\\Y\end{smallmatrix}\triangleleft\begin{smallmatrix}X'\\Y'\end{smallmatrix}\right)$

sequential split



$L\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};\begin{smallmatrix}X\\Y\end{smallmatrix}\otimes\begin{smallmatrix}X'\\Y'\end{smallmatrix}\right)$

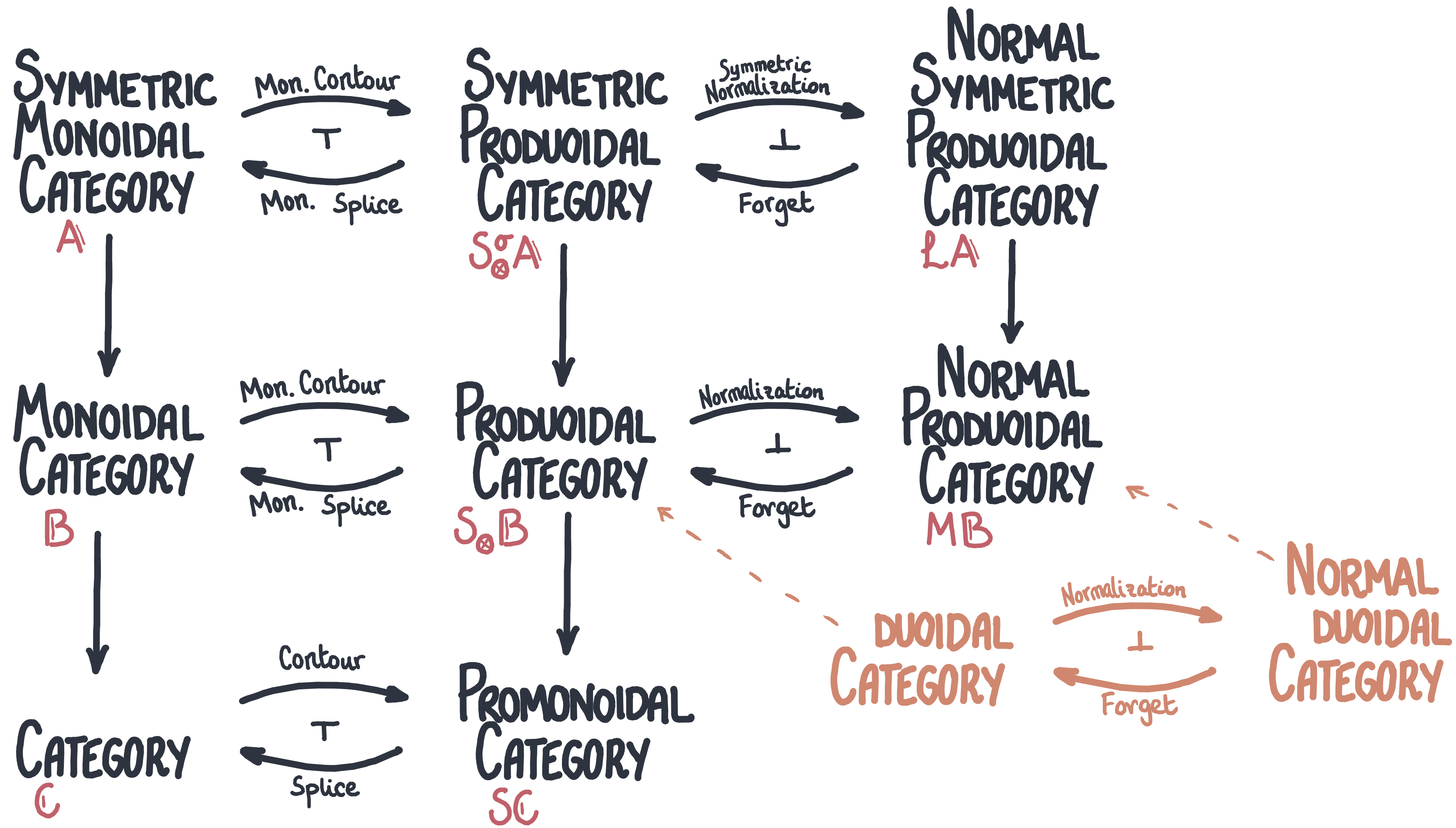
parallel split

$L\mathbb{C}\left(\begin{smallmatrix}A\\B\end{smallmatrix};N\right)$

sequential unit

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

Recap



Symmetric Monoidal Category
A
Mon. Contour
⊤
Mon. Splice
Symmetric Produoidal Category
$S_{\otimes}^{\sigma}A$
Symmetric Normalization
⊥
Forget
Normal Symmetric Produoidal Category
$\mathcal{L}A$
Monoidal Category
B
Mon. Contour
⊤
Mon. Splice
Produoidal Category
$S_{\otimes}B$
Normalization
⊥
Forget
Normal Produoidal Category
$\mathcal{M}B$
Category
C
Contour
⊤
Splice
Promonoidal Category
SC
Duoidal Category
Normalization
⊥
Forget
Normal Duoidal Category

Part 7: Session Types

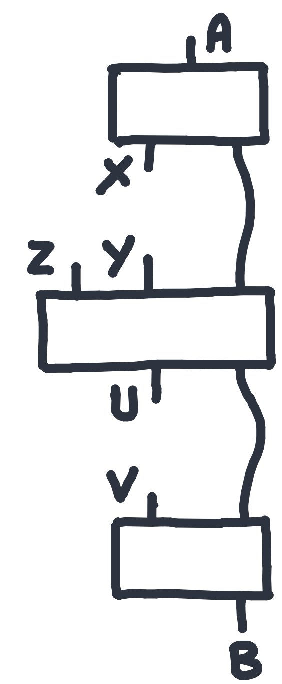
Session Types

Honda et al.

! Send
? Receive

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

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



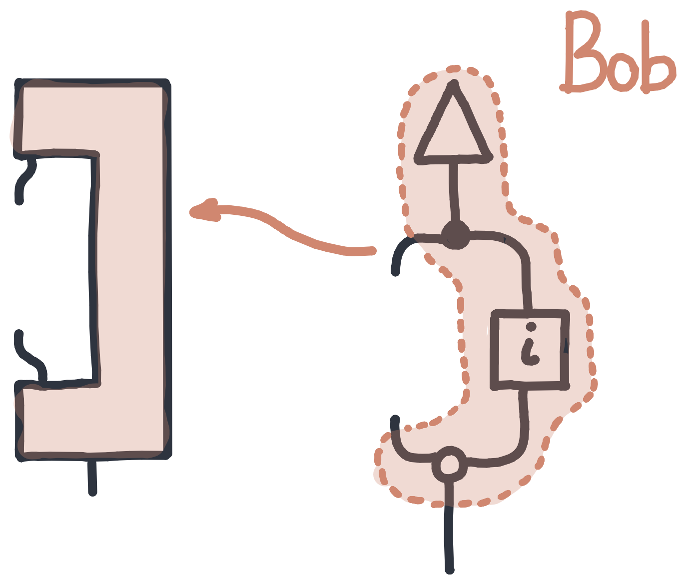
Proposition. The $\otimes$ of lenses is representable. Lenses are monoidal with $\binom{X}{Y}\otimes\binom{X'}{Y'} = \binom{X\otimes X'}{Y\otimes Y'}$.

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

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

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

ONE-TIME PAD



$\text{Bob} : \mathrm{LDist}(I \to B \,;\, !B \triangleleft ?B)$

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

We can finally type pieces of a morphism and compose them via the laxators of a produoidal category, or simply by string diagrams.

Some References

- Garner, López Franco. Commutativity.
- Melliès, Zeilberger. Parsing as a lifting problem.
- Pastro, Street. Doubles for monoidal categories.
- Booker, Street. Tannaka duality and convolution for duoidal categories.

- Earnshaw, Hefford, Román. The Produoidal Algebra of Process Decomposition.
- Román. Open Diagrams via Coend Calculus.

END

Relation to: Wiring Diagrams

Spivak, Vasilakopoulou, Rupel, ...

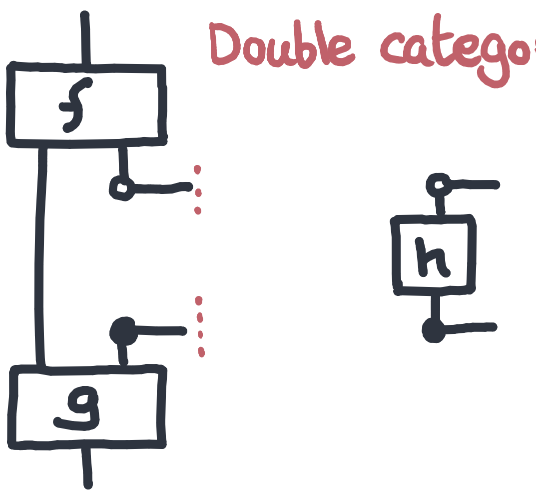
There is a procedure that, from a normal symmetric produoidal extracts a symmetric multicategory: it forgets dependency.

$$
\begin{tikzcd}
 & \mathbb{V}(A; B \triangleleft C) \arrow[dr] \arrow[dd, phantom, "<"] & \\
\mathbb{V}(A; B \otimes C) \arrow[ur] \arrow[dr] & & \mathbb{V}(A; B \boxtimes C) \\
 & \mathbb{V}(A; C \triangleleft B) \arrow[ur] &
\end{tikzcd}
$$

- The multicategory of wiring diagrams is the normal symmetric produoidal of lenses, after forgetting dependency.

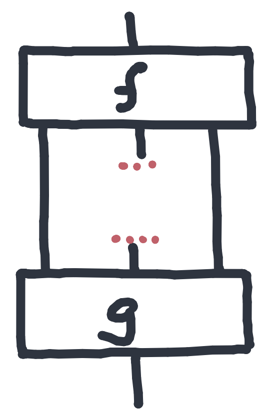
Relation to: Cornering Diagrams

We can also split processes in the free proarrow equipment.



Double categorical cells.

Limited to the symmetric case. The following is not expressible.



THM (Nester, Boisseau, Román). In the symmetric case, contexts and one-sided cornering cells coincide. Thus, they form the free normal symm. cofree produoidal.

Relation to: Linearly Distrib. Cats.

Linear actegories provide semantics for concurrency. Can we compare?

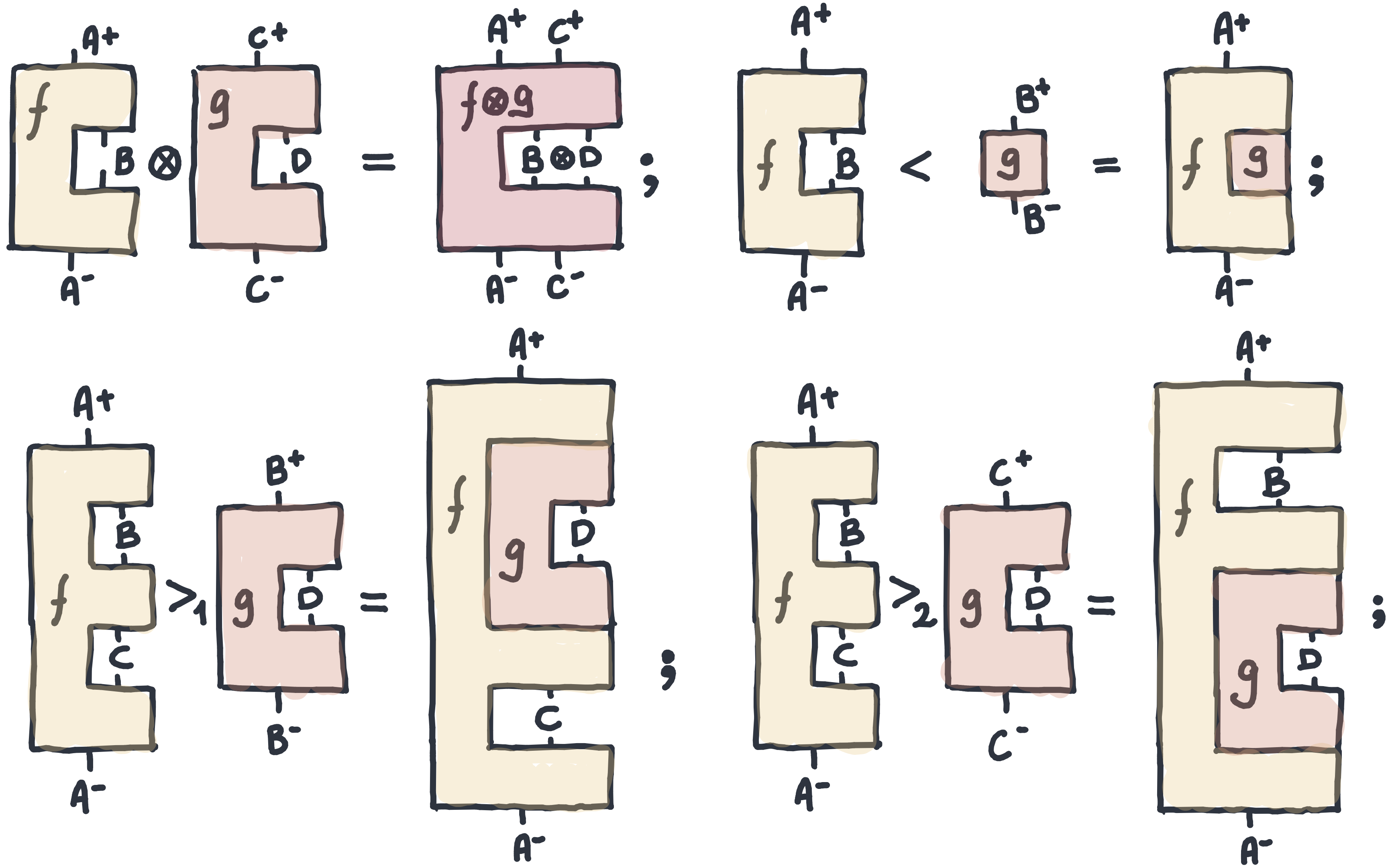
- Types track polarities assigned by the user, instead of send/receive.
- Much richer structure: choice, fixpoints, ...

Surprisingly, there is some clear mathematical connection.

CONJECTURE. Isomix categories are normal duoidal categories.
A normal duoidal $(\mathbb{C}, *, \triangleleft, N)$ is isomix $(\mathbb{C}, \otimes = *, \parr = \triangleleft, N)$.

Cockett (et al); Blute, Cockett, Seely

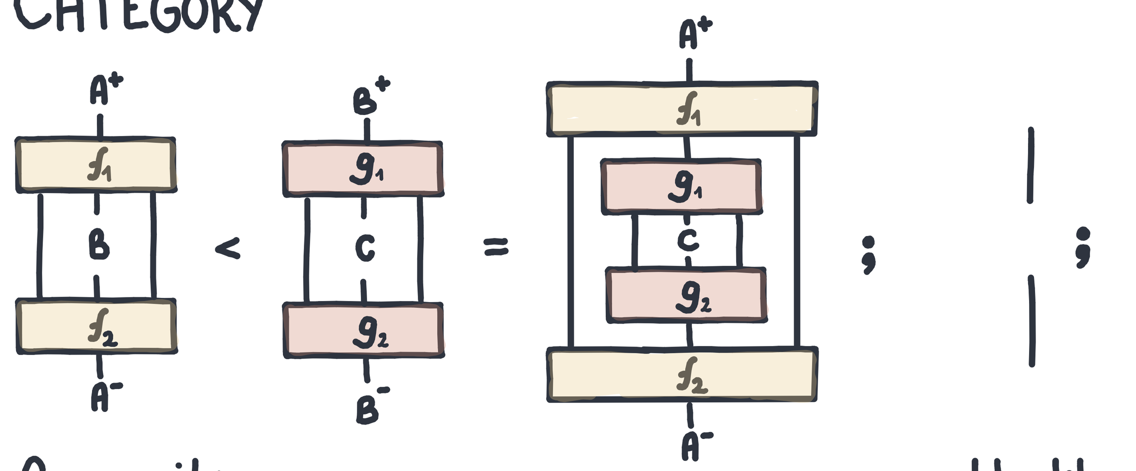
Algebra of Lenses



Produoidal Algebra of Monoidal Contexts

Earnshaw, Hefford, Román.

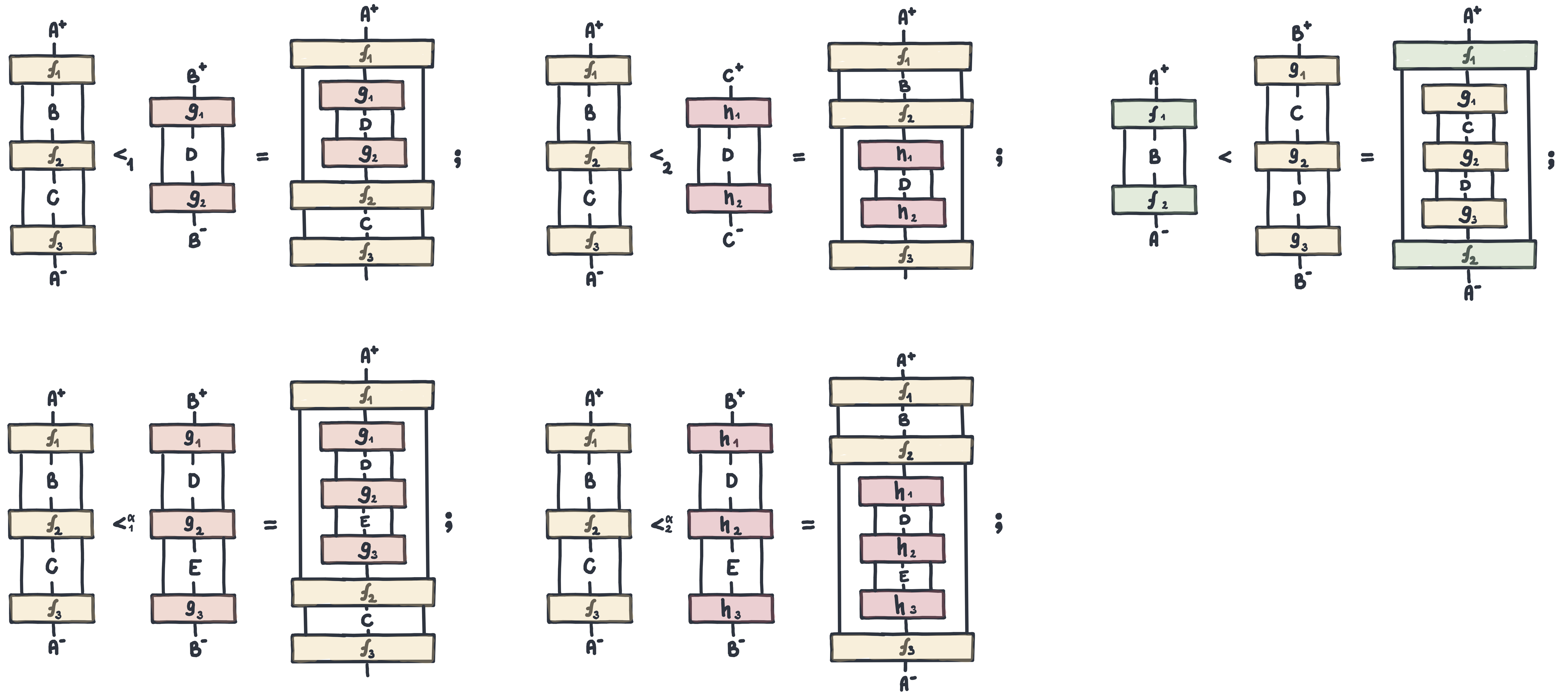
Category



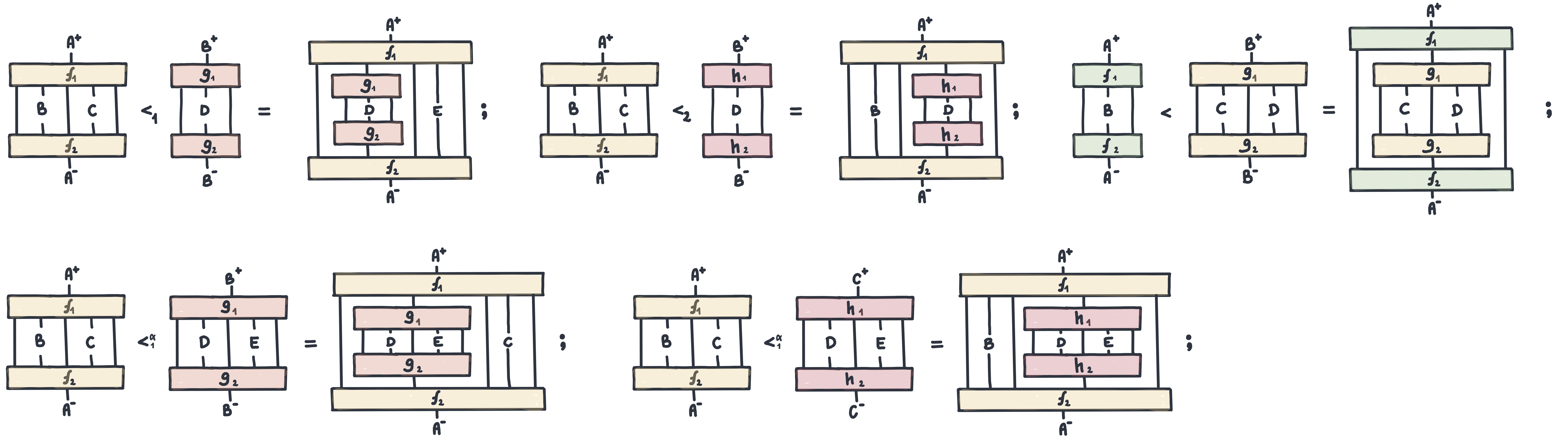
Composition

Identity

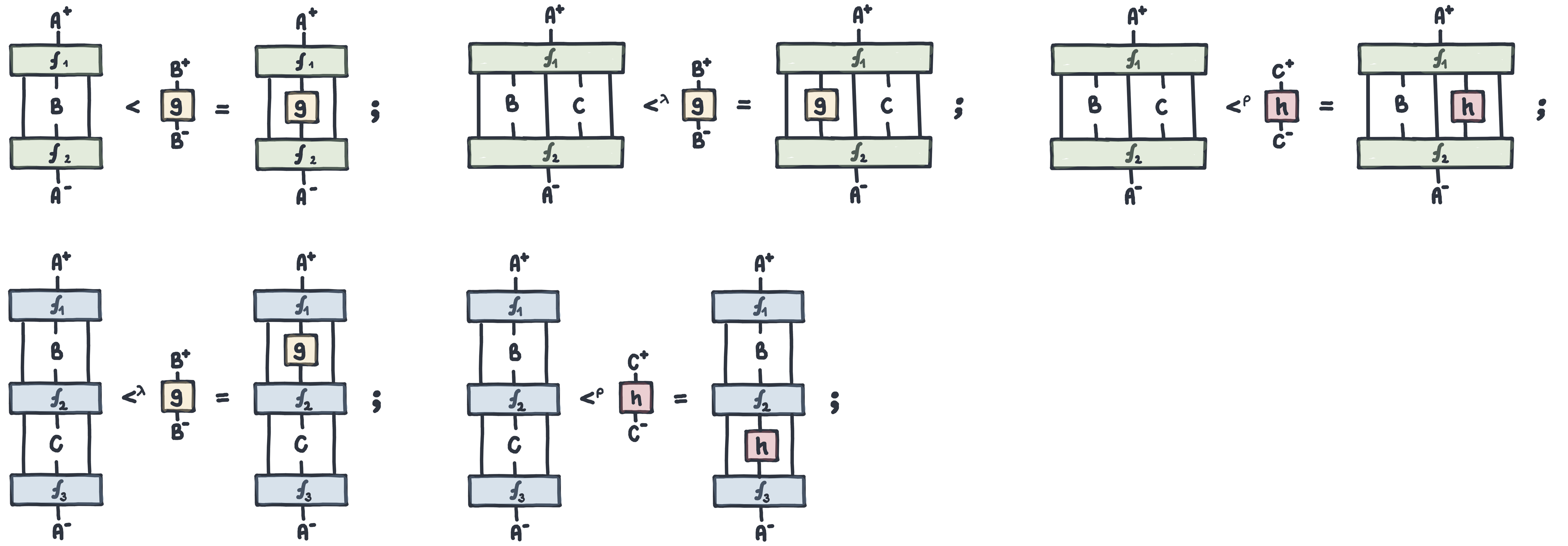
Sequential Protensor



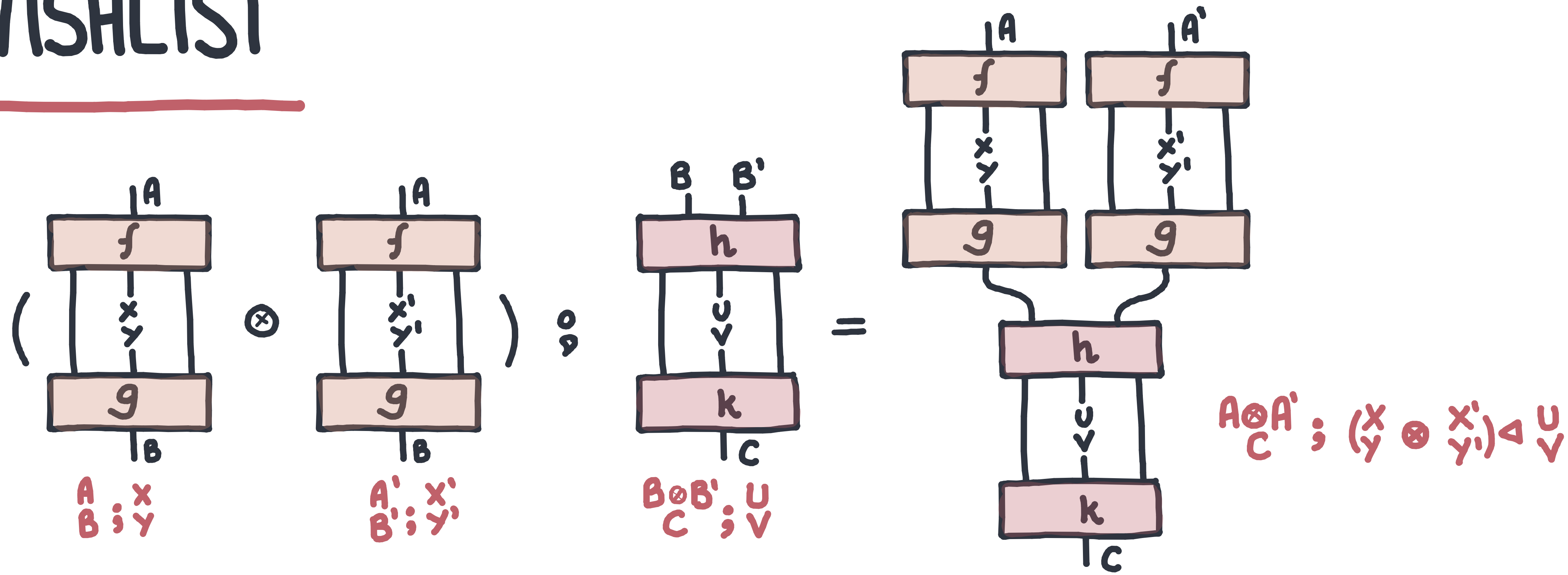
Parallel Protensor



Unit



WISHLIST



Algebra of parallel/sequential decomposition. (Pro) duoidal categories.

Semantics of incomplete diagrams. Monoidal context.

Message-passing. Send-Receive types.

Endorelations in a Monoid

Let M be any monoid. Endorelations form a duoidal poset. Commutative if M is.

$$R \triangleleft S\,(x,y) = \exists z.\, R(x,z) \wedge S(z,y), \qquad N(x,y) = (x=y),$$
$$R \otimes S\,(x,y) = \exists x_1,x_2.\, (x = x_1 x_2) \wedge R(x_1,y_1) \wedge S(x_2,y_2) \wedge (y_1 y_2 = y), \qquad I(x,y) = (x=e=y).$$

For instance the first laxator says

$$(R \triangleleft S) \otimes (R' \triangleleft S')\,(x,y) = \exists x_1 x_2 y_1 y_2 z_1 z_2.\; x = x_1 x_2 \wedge \begin{array}{l} R(x_1;z_1) \wedge S(z_1;y_1) \\ R(x_2;z_2) \wedge S(z_2;y_2) \end{array} \wedge y_1 y_2 = y.$$

$$\rightarrow \exists x_1 x_2 y_1 y_2 \begin{array}{l} z_1' z_2' \\ z_1 z_2 \end{array}.\; x = x_1 x_2 \wedge \begin{array}{l} R(x_1;z_1) \\ R(x_2;z_2) \end{array} \wedge z_1 z_2 = z_1' z_2' \wedge \begin{array}{l} S(z_1';y_1) \\ S(z_2';y_2) \end{array} \wedge y_1 y_2 = y.$$

Normalization gives affine relations or biaffine relations.

PROFUNCTORS

DEFINITION. A profunctor $P : \mathbb{C} \nrightarrow \mathbb{D}$ is a functor
$$P : \mathbb{C}^{op} \times \mathbb{D} \to \mathrm{SET}.$$

Equivalently, a family of sets $P(X;Y)$ indexed by objects $X \in \mathbb{C}$ and $Y \in \mathbb{D}$ and with actions
$$(>) : \hom(X';X) \times P(X;Y) \to P(X';Y),$$
$$(<) : P(X;Y) \times \hom(Y;Y') \to P(X;Y'),$$
that are functorial:
$$f > (p < g) = (f > p) < g$$
$$f_0 > f_1 > p = (f_0 ⨾ f_1) > p$$

Profunctors compose via coends
$$(P ⨾ Q)(X;Z) = \int^{Y \in \mathbb{B}} P(X;Y) \times Q(Y;Z)$$
$$= \coprod_{Y \in \mathbb{B}} P(X;Y) \times Q(Y;Z) \Big/ \sim_D .$$

Normalizing Duoidals

Consider a duoidal category $(\mathbb{V}, \otimes, I, \triangleleft, N)$. If we want a normal category, we need to change $\otimes$ so that N is a unit.

- N is already a $\otimes$-monoid, with $N \otimes N \to N$ and $I \to N$.
- The category of $N^{\otimes}$-bimodules is monoidal:

$$N \otimes (A \triangleleft B) \otimes N \to (N \triangleleft N) \otimes (A \triangleleft B) \otimes (N \triangleleft N) \to (N \otimes A \otimes N) \triangleleft (N \otimes B \otimes N) \to A \triangleleft B,$$

but duoidality requires reflexive coequalizers to define the new tensor $(\otimes_N)$, and these coequalizers need to be preserved by $(\otimes)$,

$$A \otimes N \otimes B \rightrightarrows A \otimes B \twoheadrightarrow A \otimes_N B.$$

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

NORMALIZING PRODUOIDALS

Normalization works always in produoidals.

Consider a produoidal category $(\mathbb{V}, \otimes, I, \triangleleft, N)$. We can ALWAYS (!) normalize it. There is a "bimodule promonad", and its category gives a normalization.

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

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

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

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

THEOREM (EHR23). Let $(\mathbb{V}, \otimes, I, \triangleleft, N)$ a produoidal category. Then, $(\mathcal{N}_\sigma\mathbb{V}, \otimes_N, \triangleleft_N, N)$ is a normal produoidal. Moreover, $\mathcal{N}$: Produo $\to$ Produo.

THEOREM (EHR23). Let $(\mathbb{V}, \otimes, I, \triangleleft, N)$ a symm. produoidal category. Then, $(\mathcal{N}_\sigma\mathbb{V}, \otimes_N, \triangleleft_N, N)$ is a normal sym produoidal. Moreover, $\mathcal{N}_\sigma$: Produo $\to$ Produo.

Normalizing Symmetric Duoidals

Consider a $\otimes$-sym. duoidal category $(\mathbb{V}, \otimes, I, \triangleleft, N)$. If we want a normal category, we need to change $\otimes$ so that N is a unit.

- N is already a $\otimes$-monoid, with $N \otimes N \to N$ and $I \to N$.
- The category of $N^{\otimes}$-modules is monoidal:

$$N \otimes (A \triangleleft B) \to (N \triangleleft N) \otimes (A \triangleleft B) \to (N \otimes A) \triangleleft (N \otimes B) \to A \triangleleft B,$$

but duoidality requires reflexive coequalizers to define the new tensor $(\otimes_N)$, and these coequalizers need to be preserved by $(\otimes)$,

$$A \otimes N \otimes B \rightrightarrows A \otimes B \twoheadrightarrow A \otimes_N B.$$

THEOREM (Garner, López Franco). Let $(\mathbb{V}, \otimes, I, \triangleleft, N)$ a $\otimes$-sym. duoidal with reflexive coequalizers, preserved by $(\otimes)$. Then, $(\mathrm{Mod}_N^{\otimes}, \otimes_N, N, \triangleleft, N)$ is a normal $\otimes$-sym. duoidal.