A Foundation for Ledger Systems

Chad Nester[1]

Tallinn University of Technology

Tokenomics 2020 – 27/10/20

[1]This research was supported by the ESF funded Estonian IT Academy research measure (project 2014-2020.4.05.19-0001).

What is This?

Distributed ledger = Consensus + Ledger

This talk: algebra of ledgers is monoidal categories.

Symmetric monoidal category $\leftrightsquigarrow$ notion of ledger.

What is Algebra?

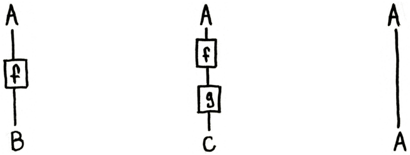
Obviously "$7 + 3$" and "$3 + 7$" are different.

Algebra: $7 + 3 = 10 = 3 + 7$.

Different ways to construct the same number.

What The Heck is a Symmetric Monoidal Category?

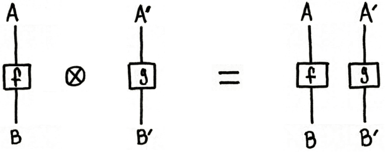
A **Category** consists of **Objects** $A, B, C, \ldots$ and **Morphisms** $f, g, \ldots$ with a **Source** and **Target** $A \xrightarrow{f} B$.



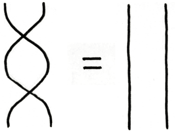
If the target of $A \xrightarrow{f} B$ is the source of $B \xrightarrow{g} C$ we may **Compose** f and g to form $A \xrightarrow{fg} C$.

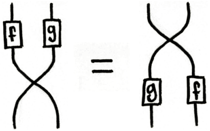
What The Heck is a Symmetric Monoidal Category?

A strict **Monoidal Category** is a category with a binary operation $\otimes$ that works on objects – $A \otimes B$ – and on morphisms, as in:



which satisfies a few axioms. A strict monoidal category is **Symmetric** in case there are well-behaved maps $A \otimes B \to B \otimes A$:





Monoidal Categories as Resource Theories

Monoidal categories are like theories of **resource convertibility**.

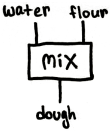
$$\text{Objects} \leftrightsquigarrow \text{Resources}$$

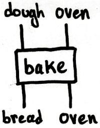
$$\text{Morphisms} \leftrightsquigarrow \text{Transformations}$$

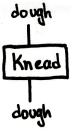
For Example, objects generated by:

$$\{\texttt{bread}, \texttt{dough}, \texttt{water}, \texttt{flour}, \texttt{oven}\}$$

and morphisms generated by:

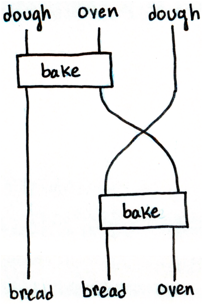






Monoidal Categories as Resource Theories

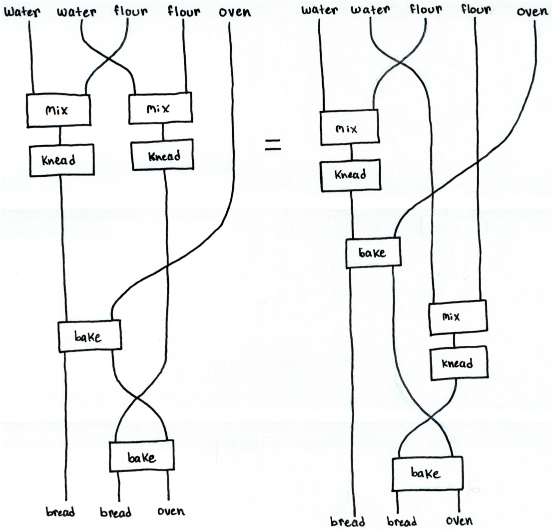
Then morphisms are things like:



which describes baking two loaves of bread in sequence.

Monoidal Categories as Resource Theories

Equality indicates that two processes *have the same effect*. e.g.,



Ledgers and Material History

String diagrams $\leftrightsquigarrow$ **Material Histories**.

Ledgers (and **Transactions**) $\leftrightsquigarrow$ Material Histories.

Add transactions to ledger by **Composition**.

Equal Transactions (Ledgers) $\leftrightsquigarrow$ Same Effect (Current State).

Modelling Ownership

We care about **Ownership**. Let's model that.

This works for an arbitrary resource theory.

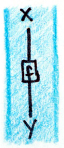
We assume a set $\mathcal{C} = \{\texttt{Alice}, \texttt{Bob}, \texttt{Carol}, \ldots\}$ of possible owners, each of which we associate with a colour:

Modelling Ownership

Objects are like $X^{\texttt{Alice}}$, $Y^{\texttt{Bob}}$, $X^{\texttt{Alice}} \otimes Y^{\texttt{Bob}}, \ldots$

$X^{\texttt{Alice}}$ is an X **owned by** `Alice`.

Morphisms are like $f^{\texttt{Alice}} : X^{\texttt{Alice}} \to Y^{\texttt{Alice}}$.



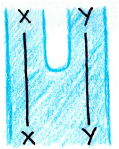
$f^{\texttt{Alice}}$ is `Alice` transforming **her** resources.

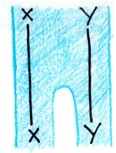
Modelling Ownership

Two 1$ coins versus one 2$ coin. Operational difference.

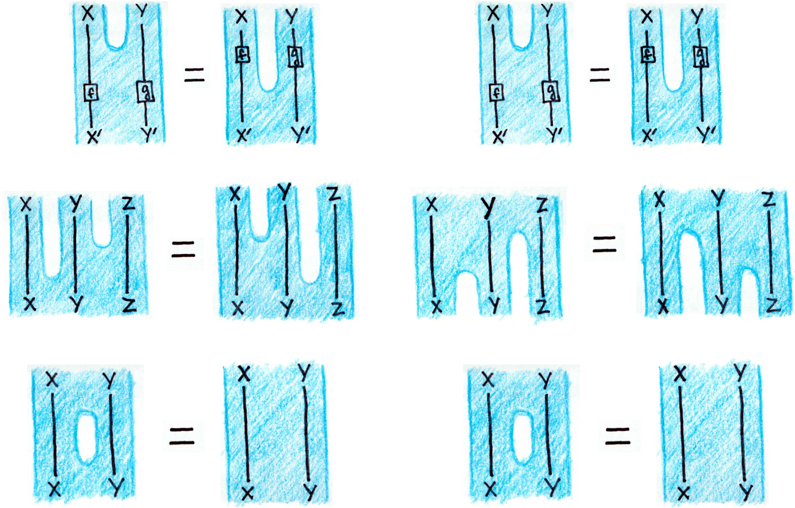
$$\phi^{\texttt{Alice}}_{X,Y} : X^{\texttt{Alice}} \otimes Y^{\texttt{Alice}} \to (X \otimes Y)^{\texttt{Alice}}$$

$$\psi^{\texttt{Alice}}_{X,Y} : (X \otimes Y)^{\texttt{Alice}} \to X^{\texttt{Alice}} \otimes Y^{\texttt{Alice}}$$





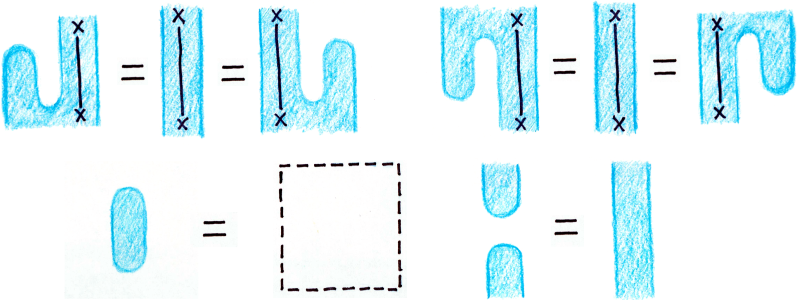
Modelling Ownership



Modelling Ownership

Also, empty collections:

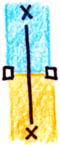
$$\phi_0 : I \to I^{\texttt{Alice}} \qquad \psi_0 : I^{\texttt{Alice}} \to I$$



Change of Ownership

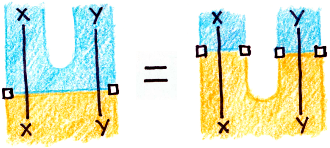
The owner of a thing can **Change**:

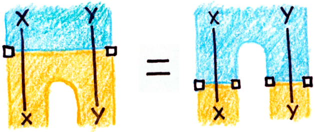
$$\gamma_X^{\texttt{Alice},\texttt{Bob}} : X^{\texttt{Alice}} \to X^{\texttt{Bob}}$$

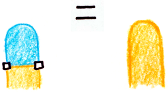


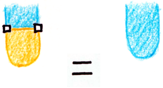
for each $\texttt{Alice}, \texttt{Bob} \in \mathcal{C}$ and X of $\mathbb{X}$.

Change of Ownership

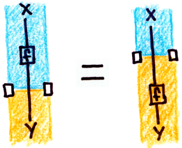


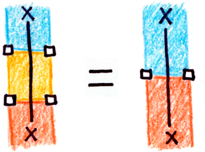


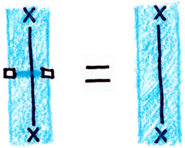




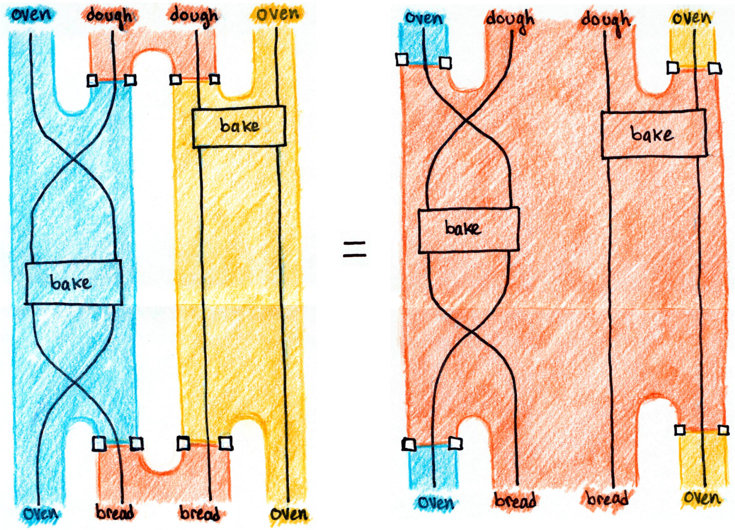
Change of Ownership







Change of Ownership



Pictures of What?

$\mathbb{X}$ a resource theory, $\mathcal{C}$ colours, define $\mathcal{C}(\mathbb{X})$ to be $\mathbb{X} \times \mathcal{C}$ plus

$$\frac{A \in \mathcal{C} \qquad X, Y \text{ objects of } \mathbb{X}}{\phi^A_{X,Y} : X^A \otimes Y^A \to (X \otimes Y)^A \text{ in } \mathcal{C}(\mathbb{X})} \qquad \frac{A \in \mathcal{C}}{\phi^A_I : I \to I^A \text{ in } \mathcal{C}(\mathbb{X})}$$

$$\frac{A \in \mathcal{C} \qquad X, Y \text{ objects of } \mathbb{X}}{\psi^A_{X,Y} : (X \otimes Y)^A \to X^A \otimes Y^A \text{ in } \mathcal{C}(\mathbb{X})} \qquad \frac{A \in \mathcal{C}}{\psi^A_I : I^A \to I \text{ in } \mathcal{C}(\mathbb{X})}$$

$$\frac{A, B \in \mathcal{C} \qquad X \text{ an object of } \mathbb{X}}{\gamma^{A,B}_X : X^A \to X^B \text{ in } \mathcal{C}(\mathbb{X})}$$

Subject to 18 equations.

Math Facts

$\mathcal{C}(\mathbb{X})$ is largely characterized by:

Proposition

For any symmetric monoidal category $\mathbb{X}$ and any set $\mathcal{C}$, there is a strong symmetric monoidal functor

$$A : \mathbb{X} \to \mathcal{C}(\mathbb{X})$$

for each $A \in \mathcal{C}$. Further, there is a monoidal and comonoidal natural transformation

$$\gamma^{A,B} : A \to B$$

between the functors corresponding to any two $A, B \in \mathcal{C}$.

Pictures of What?

In fact, we have the following:

Proposition

There is an adjoint equivalence between $\mathbb{X}$ and $\mathcal{C}(\mathbb{X})$ for each functor corresponding to some $A \in \mathcal{C}$.

This means $\mathbb{X}$ and $\mathcal{C}(\mathbb{X})$ have the same categorical structure.

Point of interest: while our final two axioms concerning the γ-maps are motivated by our desire to model ownership, they are precisely what is needed for this proposition.

No More Slides

Thanks for Listening!