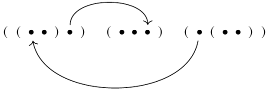
# The structure of coherence for unbiased untyped conjunction

Peter M. Hines — University of York

**LambdaComb Group Meeting**

Paris – Sorbonne Jan. 2024



Au fond de l'Inconnu pour trouver du nouveau!

# Objective of the talk(!)

We will revisit some classic & well-established category theory (coherence & strictification for associativity)

**Motivation** We often ignore the structure of coherence & work in the "strict" setting

**Simple Question** Do we miss anything interesting, by doing so?

**Our claim :**

We can see categorical coherence as a **concrete tool** in a wide range of topics, from *combinatorics* & *number theory* to *algebra*, *cryptography*, and *computability*.

Further, interpreting such topics via category theory allows us to make non-trivial connections between them.

# The structure of the talk

1. Basic definitions & properties relating to coherence.
2. What they look like in the untyped (i.e. single-object, or monoid-theoretic case).
   - Coherence for associativity as pure algebra.
   - Why there is only one interesting case(!)
     and where else we see it.
3. The unbiased setting (a tensor of every arity).
   - Coherence, strictification, reduction to the usual setting.
   - The untyped setting.
   - Why we should care ...

**Throughout the talk ...**

A series of conjectures / open questions / random ideas . . .

# The very basics

A **(semi-monoidal) tensor** on a category $\mathcal{C}$ is a *monoidal tensor* w.o. an explicit unit.

A **functor** $\_ \otimes \_ : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$ equipped with a (semi-monoidal) **natural isomorphism**

$$\alpha \ : \ (\_ \otimes (\_ \otimes \_)) \ \Rightarrow \ ((\_ \otimes \_) \otimes \_)$$

that satisfies *"a notion of coherence"*.

**Very informally(!)**

Any two ways of performing the same rebracketing are the same.

A *necessary and sufficient* condition is **MacLane's pentagon**.

For all objects $(X, Y, Z, T) \in Ob(\mathcal{C} \times \mathcal{C} \times \mathcal{C} \times \mathcal{C})$,
the components of the natural iso. $\alpha$ satisfy :

$$\alpha_{X \otimes Y, Z, T} \, \alpha_{X, Y, Z \otimes T} \ = \ (\alpha_{X,Y,Z} \otimes Id_T) \alpha_{X, Y \otimes Z, T} (Id_X \otimes \alpha_{Y,Z,T})$$

# Why we don't really care :)

A tensor $\_\otimes\_$ is **strict** when the natural isomorphism mediating associativity

$$\alpha : (\_\otimes(\_\otimes\_)) \Rightarrow ((\_\otimes\_)\otimes\_)$$

is the identity, in which case all its components are identity arrows.

**Informally, again ...**

In the strict case, we do not need to consider bracketings.

**Theorem** (MacLane) Every category with a tensor is (semi-monoidally) equivalent to a category with a **strict** tensor.

**Practically**

In day-to-day working, we ignore entirely questions of

1. bracketings
2. coherence isomorphisms

# A relevant quotation!

MONOIDAL CATEGORIES : A Unifying Concept
in Mathematics, Physics, and Computing (Noson Yanofsky 2023)

"**The above theorem is subtle**. *Most people use this fact so as not to worry that the tensor in their favorite category is not strictly associative. The reasoning is that all 'mathematically relevant' properties are preserved . . . hence, they might as well use the properties of the strict monoidal category.*

*Peter Freyd describes what properties are preserved [by equivalences] in the category of categories. We are asking about the 2-category of monoidal categories. What is exactly true about a strict monoidal category and not true about its equivalent [non-strict] monoidal category?*

**As far as I know, no one has worked out the details of this. It is worthy of further study.**

# Some low-hanging fruit

Let $\_ \otimes \_$ be a tensor on a small category $\mathcal{M}$.

We say that $(M, \otimes)$ **untyped** when it has precisely one object[1].

Algebraically, $\mathcal{M}$ is a monoid, and the tensor

$$\_ \otimes \_ : \mathcal{M} \times \mathcal{M} \to \mathcal{M}$$

is a homomorphism.

**Proposition :**

The following are equivalent :

1. $(\mathcal{M}, \otimes)$ is monoidal (rather than semi-monoidal).
2. $\mathcal{M}$ is the endomorphism monoid of a unit object.
3. $\_ \otimes \_$ is strictly associative.

[1] The cardinality of $Ob(\mathcal{M})$ is certainly not preserved by equivalences of categories!

# An important special case:

**Proposition:**

$$(\_ \star \_) : \mathcal{M} \times \mathcal{M} \hookrightarrow \mathcal{M} \text{ is strictly associative}$$

$$\Longleftrightarrow$$

The unique object of $\mathcal{M}$ is the unit object.

**Proof** ($\Leftarrow$) *[Standard Theory ...]*

By the Eckmann-Hilton argument on the interchange law, the endomorphism monoid of a unit object is abelian, and the tensor and composition coincide.

# Is it because $I$ is strict?

**Proof** ($\Rightarrow$) *[Journal Homotopy & Related Structures PMH 2016]*

Define an injective monoid endomorphism by :

$$\eta = (1 \star \_ \star 1) : \mathcal{M} \hookrightarrow \mathcal{M}$$

Define a semi-monoidal tensor on its image $\eta(\mathcal{M})$ by, for all $\eta(r), \eta(s) \in \eta(\mathcal{M})$

$$\eta(r) \odot \eta(s) = 1 \star (r \star s) \star 1$$

By construction, $(\mathcal{M}, \star) \cong (\eta(\mathcal{M}), \odot)$.

Observe : the unique objects of both $(\mathcal{M}, \star)$ and $(\eta(\mathcal{M}), \odot)$ are **pseudo-idempotent**.

**Reminder . . .**

A *pseudo-idempotent* object of a semi-monoidal category is one satisfying $U \cong U \otimes U$

# The final step

By definition, for all $\eta(f) \in \eta(\mathcal{M})$,

$$\begin{aligned} 1 \odot \eta(f) &= 1 \star (1 \star f) \star 1 \\ &= 1 \star 1 \star f \star 1 \\ &= 1 \star f \star 1 \\ &= \eta(f) \end{aligned}$$

Thus $1 \odot \_ = Id_{\eta(\mathcal{M})} = \_ \odot 1$.

The unique object of $(\eta(\mathcal{M}), \odot)$ is a **cancellative pseudo-idempotent**!

Similarly, of course, for $(\mathcal{M}, \star)$.

Now recall A. Saavedra's characterisation of unit objects as *cancellative pseudo-idempotents*.

- *Catégories Tannakiennes* A. Saavedra (1972)
- *Elementary Remarks on Units* J. Kock (2008)
- *Coherence for Weak Units* A. Joyal, J. Kock (2011)

# A “folklore” result

What we have in the non-strict case (e.g. Lambek & Scott’s C-monoids) :

**Theorem :**

Let $\_ \star \_ : \mathcal{M} \times \mathcal{M} \rightarrow \mathcal{M}$ be a tensor on a (non-abelian) monoid.

The canonical associativity isomorphisms for $\_ \star \_$ form a group,

isomorphic to **Richard Thompson’s group** $\mathcal{F}$.

**Proof ?** Rediscovered *many times*! Known to R. Thompson et al. (1970s ?)

- (Incomplete) historical account & outline proof (PMH 2023)
- First fully explicit proof by P. Dehornoy
  *“The structure group for the associativity identity” (1996)*
- An explicit tensor on $\mathcal{F}$ given (purely algebraically) by K Brown
  *“The homology of Thompson’s $\mathcal{F}$” (2004)*

# The structure of $\mathcal{F}$

Thompson's $\mathcal{F}$ is defined by :

**Elements** (Equivalence classes of) pairs of binary trees $(S, T)$ where $S$ and $T$ have the *same number of leaves*.

**The Equivalence** The smallest equivalence relation satisfying :

$(T, S) \sim (V, U)$ if we can derive both

1. $V$ from $T$
2. $U$ from $S$

by "pasting some binary tree $X$ onto the same leaf of both $T$ and $S$".

**Composition** This is determined by $[T, S]_\sim \, [S, R]_\sim \; = \; [T, R]_\sim$

**Identity & Inverses** $[T, T]$ is always the identity, and $[T, U]^{-1} = [U, T]$.

**There are *many* other equivalent descriptions of $\mathcal{F}$**

e.g. M. V. Lawson's 2006 description as *linear clauses* using the clause algebra of unification & resolution from Girard's Geometry of Interaction (III)

# The structure of $\mathcal{F}$

Thompson's $\mathcal{F}$ is defined by :

**Elements** (Equivalence classes of) pairs of binary trees $(S, T)$ where $S$ and $T$ have the *same number of leaves*.

**The Equivalence** The smallest equivalence relation satisfying :

$(T, S) \sim (V, U)$ if we can derive both

1. $V$ from $T$
2. $U$ from $S$

by "pasting some binary tree $X$ onto the same leaf of both $T$ and $S$".

**Composition** This is determined by $[T, S]_\sim \, [S, R]_\sim \; = \; [T, R]_\sim$

**Identity & Inverses** $[T, T]$ is always the identity, and $[T, U]^{-1} = [U, T]$.

There are *many* other equivalent descriptions of $\mathcal{F}$

e.g. M. V. Lawson's 2006 description as *linear clauses* using the clause algebra of unification & resolution from Girard's Geometry of Interaction (III)

# The structure of $\mathcal{F}$

Thompson's $\mathcal{F}$ is defined by :

**Elements** (Equivalence classes of) pairs of binary trees $(S, T)$ where $S$ and $T$ have the *same number of leaves*.

**The Equivalence** The smallest equivalence relation satisfying :

$(T, S) \sim (V, U)$ if we can derive both

1. $V$ from $T$
2. $U$ from $S$

by "pasting some binary tree $X$ onto the same leaf of both $T$ and $S$".

**Composition** This is determined by $[T, S]_\sim \, [S, R]_\sim \; = \; [T, R]_\sim$

**Identity & Inverses** $[T, T]$ is always the identity, and $[T, U]^{-1} = [U, T]$.

**There are *many* other equivalent descriptions of $\mathcal{F}$**

e.g. M. V. Lawson's 2006 description as *linear clauses* using the clause algebra of unification & resolution from Girard's Geometry of Interaction (III)

# The structure of $\mathcal{F}$

Thompson's $\mathcal{F}$ is defined by :

**Elements** (Equivalence classes of) pairs of binary trees $(S, T)$ where $S$ and $T$ have the *same number of leaves*.

**The Equivalence** The smallest equivalence relation satisfying :

$(T, S) \sim (V, U)$ if we can derive both

1. $V$ from $T$
2. $U$ from $S$

by "pasting some binary tree $X$ onto the same leaf of both $T$ and $S$".

**Composition** This is determined by $[T, S]_\sim \, [S, R]_\sim \; = \; [T, R]_\sim$

**Identity & Inverses** $[T, T]$ is always the identity, and $[T, U]^{-1} = [U, T]$.

There are *many* other equivalent descriptions of $\mathcal{F}$

e.g. M. V. Lawson's 2006 description as *linear clauses* using the clause algebra of unification & resolution from Girard's Geometry of Interaction (III)

# The structure of $\mathcal{F}$

Thompson's $\mathcal{F}$ is defined by :

**Elements** (Equivalence classes of) pairs of binary trees $(S, T)$ where $S$ and $T$ have the *same number of leaves*.

**The Equivalence** The smallest equivalence relation satisfying :

$(T, S) \sim (V, U)$ if we can derive both

1. $V$ from $T$
2. $U$ from $S$

by "pasting some binary tree $X$ onto the same leaf of both $T$ and $S$".

**Composition** This is determined by $[T, S]_\sim \, [S, R]_\sim \; = \; [T, R]_\sim$

**Identity & Inverses** $[T, T]$ is always the identity, and $[T, U]^{-1} = [U, T]$.

**There are *many* other equivalent descriptions of $\mathcal{F}$**

e.g. M. V. Lawson's 2006 description as *linear clauses* using the clause algebra of unification & resolution from Girard's Geometry of Interaction (III)

We see the key 'equivalence' illustrated in José Burillo's "An introduction to Thompson's $\mathcal{F}$" :

is equivalent to

**An obvious operadic interpretation**

In *'some suitable operad'* $\mathcal{O}$, the quotient is the smallest equivalence satisfying,

$$(U, T) \sim (U \circ_x A, V \circ_x A) \quad \text{for all} \quad U, V \in \mathcal{O}_n\ ,\ x \leqslant n \ \text{ and } \ A \in \mathcal{O}$$

We will consider this equivalence in other operads ...

# A key fact :

**Theorem :** (M. Brinn, C. Squier 1985) Thompson's $\mathcal{F}$ has no non-abelian quotients.

## Categorical Interpretation

For associativity in the untyped setting, there are two options :

The "free" case Canonical isomorphisms form a copy of $\mathcal{F}$

The "trivial" case Everything collapses to a monoid of 'abstract scalars'.

A conjecture on coherence for untyped associativity

# A very 'computer-science' application

- **(2004)** V. Shpilrain & G. Zapata introduce a general prescription for protocols in *non-commutative cryptography*.
- **(2006)** V. Shpilrain & A. Ushakov give the first concrete example, based on *Thompson's* $\mathcal{F}$.
- **(2007)** Ruinsky, Shamir, Tsaban comprehensively break this protocol (for the second time ... following F. Mattuci (2006))

**Conjecture [RST]**

"No cryptographic protocol based on *[coherence for untyped associativity]* can ever be secure."

**An interpretation** (PMH 2020 *Graphical Methods in Security* )

Finding Alice & Bob's private keys / shared secret in the S-U protocol is precisely *"finding the missing labels on edges in a canonical commuting diagram"*.

An ‘equivalent’ setting :

Coherence for (untyped) unbiased associativity.

# The unbiased setting

**Definition :** An **unbiased family** of tensors on a category $\mathcal{C}$ consists of

- An $\mathbb{N}^+$–indexed family of functors $\left\{ \otimes_n \ : \prod_{j=1}^{n} \mathcal{C} \rightarrow \mathcal{C} \right\}_{n>0}$ where $\otimes_1 = Id_{\mathcal{C}}$.
- A *coherent family* of natural isomorphisms.

These are usually written

$$\begin{array}{rcl} Id_C & : & \mathcal{C} \rightarrow \mathcal{C} \\ (\_ \otimes \_) & : & \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C} \\ (\_ \otimes \_ \otimes \_) & : & \mathcal{C} \times \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C} \\ (\_ \otimes \_ \otimes \_ \otimes \_) & : & \mathcal{C} \times \mathcal{C} \times \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C} \\ & \dots & \end{array}$$

Informally, 'coherence' is then the condition that any two ways of

1. rebracketing,
2. inserting brackets
3. deleting brackets

are the same.

# Equivalence with a simpler setting

Does this bring anything new???

**Theorem (T. Leinster 2009)**

Every category with a family of unbiased tensors is equivalent to one with a single strict (binary) tensor.

**Steps in Proof :**

unbiased $\longrightarrow$ binary non-strict $\longrightarrow$ strict

**Question :** Is there any reason to study unbiased tensors — untyped, or otherwise?

# A plan of action(!)

We will go in the opposite direction to T.L.'s proof :

- Start with an untyped (binary) tensor
  — a model of conjunction from categorical logic.
- Exhibit an equivalent unbiased (still untyped) version.
- Describe the structure of coherence
  — particularly, parts already known in :

  T.C.S. / logic / algebra / combinatorics / number theory.

Another conjecture, on coherence for unbiased associativity

# Uniqueness of the 'untyped' case?

The **untyped** case is based on a family of tensors on a monoid $\mathcal{M}$

$$\left\{ \star_n : \prod_{j=1}^{n} \mathcal{M} \to \mathcal{M} \right\}_{n>0\in\mathbb{N}}$$

**Conjecture** (By analogy with the binary case)

There are precisely three possibilities :

The 'strict' case The binary case $\_ \star_2 \_$ is strict iff all other tensors are strict, in which case $\mathcal{M} = \mathcal{C}(I, I)$ is uninteresting.

The 'familiar' case The binary tensor $\star_2$ is non-strict, but all $\star_n$ for $n > 2$ are given by bracketings of $\star_2$.

The 'free' case The setting we are about to describe :)

# Some motivation . . .

In the structure of coherence for untyped, unbiased tensors, we encounter :

- **Algebra** Thompson's groups $\mathcal{F}$ and $\mathcal{V}$, and their usual generalisations, Dynamical algebras, S. Kohl's 'class transposition' group, Grigorchuk's $\mathfrak{G}$, maximal prefix codes.
- **Number Theory & combinatorics** Card shuffles, Cantor spaces, Erdös's covering systems, famous integer sequences, prime factorisations, notorious number-theoretic conjectures, mixed-radix arithmetic, Conway's congruential functions.
- **Computability** / **decidability** Conway's proof of undecidability / computational universality in elementary arithmetic.
- **Several other topics(!)** . . .

**Most importantly**

The ability to relate / translate between different fields.

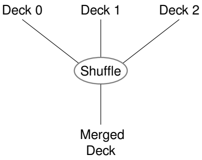
# Unbiased, untyped, tensors

$\sim$

*A combinatorial approach based on card shuffles*

# Our starting point ...

We base everything on, '**Shuffles** & **deals** of decks of cards'.




We assume all decks are *countably infinite*, and impose *two simple rules*.

1. Ordering is preserved.

   *"If card a is above card b before the shuffle,*

   *then a is still above b afterwards."*

2. The shuffle is fair(!)

   *"No cards are discarded; no 'extras' get introduced."*

# Hilbert's Hotel vs. Cantor's Casino (I)

There are two different (equivalent) ways we may model shuffles :

## The 'denotational' description, as bijections

$$(n, i) \longmapsto k$$

defined by

Card $n$ of Deck $i$ $\Downarrow$ *gets mapped to* $\Downarrow$ Position $k$ in the final deck

Define the **induced partial order** on $\overbrace{\mathbb{N} \uplus \ldots \uplus \mathbb{N}}^{k \text{ times}} = \mathbb{N} \times \{0, \ldots, k-1\}$ by

$$(x, i) \leqslant (y, j) \text{ iff } x \leqslant y \text{ and } i = j$$

**Definition** A **shuffle** is a *monotone bijection* $\psi : \mathbb{N} \uplus \ldots \uplus \mathbb{N} \rightarrow \mathbb{N}$.

# Hilbert's Hotel vs. Cantor's Casino (II)

There are two different (equivalent) ways we may model shuffles :

**The 'operational' description, as points of Cantor spaces**

Consider some $\phi : \mathbb{N} \to \{0, \ldots, k-1\}$ as a 1-sided infinite string

$$\phi \ = \ \phi_0\phi_1\phi_2\phi_3\phi_4 \ldots \ \in \ \{0, \ldots, k-1\}^\omega$$

and interpret this as a step-by-step instruction

> *"On the $j^{th}$ step, take a card from the bottom of deck $j$, and place it on top of the final stack."*

**Alt. Definition** A **shuffle** is a *balanced Cantor point*; some $\phi : \mathbb{N} \to \{0, \ldots, k-1\}$ satisfying

$$\left|\phi^{-1}(i)\right| = \left|\phi^{-1}(j)\right| \quad \forall \ i, j \in \{0, \ldots k-1\}$$

peter.hines@york.ac.uk 01232 457964

Moving from a **denotational** to an **operational** picture is straightforward.

Given a monotone bijection $\psi : \mathbb{N} \times \{0, \ldots k-1\}$,

we recover a balanced Cantor point $\phi : \mathbb{N} \to \{0, \ldots, k-1\}$ by :

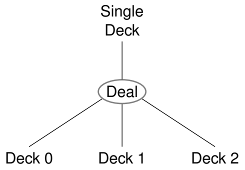
$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\psi^{-1}} & \mathbb{N} \times \{0, \ldots k-1\} \\ & \searrow^{\phi} & \downarrow \pi_2 \\ & & \{0, \ldots, k-1\} \end{array}$$

**An advantage :**

We can translate some very number-theoretic concepts
into the theory of monoids / codes / Cantor spaces, . . .

# What about *deals*??

We consider **deals** to be 'time-reversed shuffles'.




Denotationally A bijection $\lambda : \mathbb{N} \rightarrow \mathbb{N} \uplus \mathbb{N} \uplus \ldots \uplus \mathbb{N}$ whose *inverse* is monotone.

Operationally A balanced Cantor point

$$\phi = \phi_0 \phi_1 \phi_2 \phi_3 \ldots \in \{0, \ldots, k-1\}^\omega$$

with a different interpretation :

*"On the $j^{th}$ step, put the next card on top of stack number $\phi_j$."*

# Faro Shuffles & Fair Deals

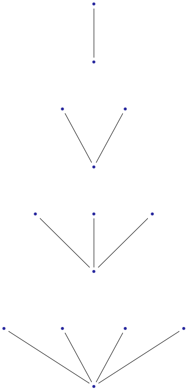
An important class of examples are the **Faro**, or (perfect) **riffle shuffles**

$\lhd_1 \ : \ \mathbb{N} \to \mathbb{N}$ $\qquad n \mapsto n$

$\lhd_2 \ : \ \mathbb{N} \uplus \mathbb{N} \to \mathbb{N}$ $\qquad (n,0) \mapsto 2n$, $(n,1) \mapsto 2n+1$

$\lhd_3 \ : \ \mathbb{N} \uplus \mathbb{N} \uplus \mathbb{N} \to \mathbb{N}$ $\qquad (n,0) \mapsto 3n$, $(n,1) \mapsto 3n+1$, $(n,2) \mapsto 3n+2$

$\lhd_4 \ : \ \mathbb{N} \uplus \mathbb{N} \uplus \mathbb{N} \uplus \mathbb{N} \to \mathbb{N}$ $\qquad (n,0) \mapsto 4n$, $(n,1) \mapsto 4n+1$, $(n,2) \mapsto 4n+2$, $(n,3) \mapsto 4n+3$



We will compose by pasting / substitution;
every **rooted planar tree** (uniquely) determines a shuffle.

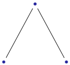
Their inverses are the **fair deals**

$\rhd_1 \ : \quad \mathbb{N} \to \mathbb{N}$



$n \mapsto n$

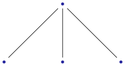
$\rhd_2 \ : \quad \mathbb{N} \to \mathbb{N} \uplus \mathbb{N}$



$n \mapsto (a, i)$ where

$n \equiv i \mod 2$ and $a = \frac{n-i}{2}$

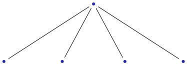
$\rhd_3 \ : \quad \mathbb{N} \to \mathbb{N} \uplus \mathbb{N} \uplus \mathbb{N}$



$n \mapsto (a, i)$ where

$n \equiv i \mod 3$ and $a = \frac{n-i}{3}$

$\rhd_4 \ : \quad \mathbb{N} \to \mathbb{N} \uplus \mathbb{N} \uplus \mathbb{N} \uplus \mathbb{N}$



$n \mapsto (a, i)$ where

$n \equiv i \mod 4$ and $a = \frac{n-i}{4}$

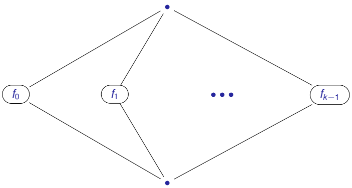
Every inverted **rooted planar tree** similarly (uniquely) determines a deal.

# Back to category theory :)

Consider the symmetric group on the natural numbers, $\mathcal{S}(\mathbb{N})$.

Define the **generalised conjunctions** to be the *unbiased family* of tensors $\left\{\star_n : \mathcal{S}(\mathbb{N})^{\times k} \hookrightarrow \mathcal{S}(\mathbb{N})\right\}_{n>0}$ given by :

$$(f_0 \star f_1 \star \ldots \star f_{k-1}) \overset{def.}{=} \lhd_k (f_0 \uplus f_1 \uplus \ldots \uplus f_{k-1}) \rhd_k$$




**The intuition :**

A pack of cards is dealt out amongst $k$ players, using a fair deal. Each player $j$ then applies $f_j$ to his stack of cards. All stacks of cards are then shuffled together using the perfect riffle shuffle.

# Some fun facts . . .

- These are all trivially functorial (group homomorphisms)

$$\lhd_k (g_0 \uplus \ldots \uplus g_{k-1}) \rhd_k \lhd_k (f_0 \uplus \ldots \uplus f_{k-1}) \rhd_k \; = \; \lhd_k (g_0 f_0 \uplus \ldots \uplus g_{k-1} f_{k-1}) \rhd_k$$

- The **binary** case is well-known; it models the *conjunction* of MELL, in Girard's first two Geometry of Interaction papers.
- We may 'compose' generalised conjunctions by substitution[2] to give
  1. 'Compound' conjunctions, e.g.

$$((\_ \star (\_ \star \_ \star \_)) \star \_) \;,\; ((\_ \star \_) \star \_ \star (\_ \star \_)) \;: \mathcal{S}(\mathbb{N})^{\times 4} \hookrightarrow \mathcal{S}(\mathbb{N})$$

  2. Unique, coherent natural isomorphisms between them :

$$((\_ \star (\_ \star \_ \star \_)) \star \_) \overset{??}{\Rightarrow} ((\_ \star \_) \star \_ \star (\_ \star \_))$$

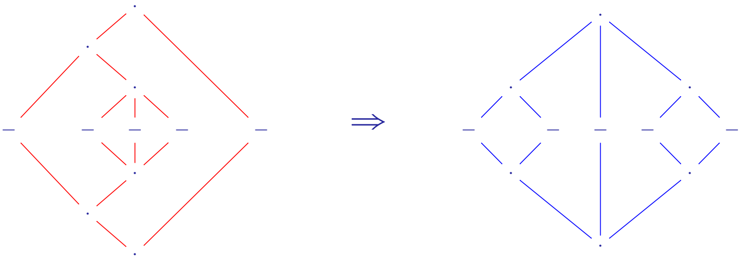
[2] Operadic composition in the endomorphism operad of $\mathcal{S}(\mathbb{N})$ in the (strictified) category of monoids with Cartesian product . . .

# Finding natural isomorphisms graphically (I)

Let us derive (the unique component of) a natural isomorphism

$$((\_ \star (\_ \star \_ \star \_)) \star \_) \;\Rightarrow\; ((\_ \star \_) \star \_ \star (\_ \star \_))$$

As **shuffles** and **deals** :



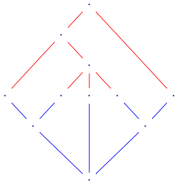
peter.hines@york.ac.uk
01232 457964

# Finding natural isomorphisms graphically (II)

Let us derive (the unique component of) a natural isomorphism

$$((\_ \star (\_ \star \_ \star \_)) \star \_) \quad \Rightarrow \quad ((\_ \star \_) \star \_ \star (\_ \star \_))$$

We find this by composing a **shuffle** and a **deal** :



$$n \mapsto \begin{cases} \frac{6n}{4} & n \equiv 0 \mod 4 \\ \frac{n}{2} + 2 & n \equiv 2 \mod 12 \\ \frac{n-2}{4} & n \equiv 6 \mod 12 \\ \frac{n}{2} - 3 & n \equiv 10 \mod 12 \\ n + 2 & n \equiv 1 \mod 2 \end{cases}$$

**The component of the nat iso. is :**

a bijection on $\mathbb{N}$, defined piece-wise linearly on modulo classes . . .

# A notion of coherence?

Defining natural isomorphisms in this way allows us to build a posetal groupoid of functors/ nat. iso.s.

**Objects** Arbitrary operadic composites of generalised conjunctions, $\mathcal{S}(\mathbb{N})^{\times k} \rightarrow \mathcal{S}(\mathbb{N})$ for all $k > 0$.

**Arrows** A single natural isomorphism between any two composites of the same arity.

## Unbiased natural iso.s

Given a series of arrows in this groupoid . . .

$$\begin{array}{cccc} T_0 & T_1 & \ldots & T_{k-1} \\ \eta_0 \Downarrow & \eta_1 \Downarrow & & \eta_{k-1} \Downarrow \\ U_0 & U_1 & \ldots & U_{k-1} \end{array}$$

# A notion of coherence?

Defining natural isomorphisms in this way allows us to build a posetal groupoid of functors/ nat. iso.s.

**Objects** Arbitrary operadic composites of generalised conjunctions, $\mathcal{S}(\mathbb{N})^{\times k} \to \mathcal{S}(\mathbb{N})$ for all $k > 0$.

**Arrows** A single natural isomorphism between any two composites of the same arity.

## Unbiased natural iso.s

. . . we have the required ‘interchange’ with gen. conjunctions.

$$\begin{array}{c} (\; T_0 \star T_1 \star \ldots \star T_{k-1} \;) \\ \Big\Downarrow {\scriptstyle (\eta_0 \star \eta_1 \star \ldots \star \eta_{k-1})} \\ (\; U_0 \star U_1 \star \ldots \star U_{k-1} \;) \end{array}$$

Equipping our posetal groupoid with a compatible family of unbiased tensors.

# Some obvious questions

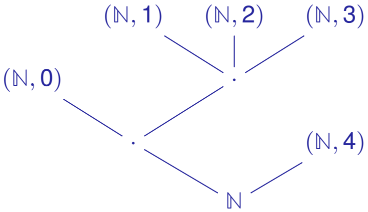
**Questions :**

- How do we derive the (unique) components of these natural iso.s,
- What is their structure?
- Are any of them *interesting*?

We now give *explicit*, *algebraic* descriptions.

# Rooted planar trees as covering systems

Let us interpret a **rooted planar tree** as a composite of Faro shuffles :




defines a bijection : $\mathbb{N} \times \{0, \ldots, 4\} \to \mathbb{N}$

Each individual deck $\mathbb{N} \times \{j\}$ is monotonically mapped to some modulo class $A_j\mathbb{N} + B_j$.

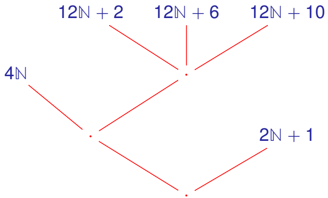
**For example :** $\mathbb{N} \times \{3\}$ is mapped onto $12\mathbb{N} + 10$.

**For arbitrary trees :**

All modulo classes are disjoint; their union is the whole of $\mathbb{N}$

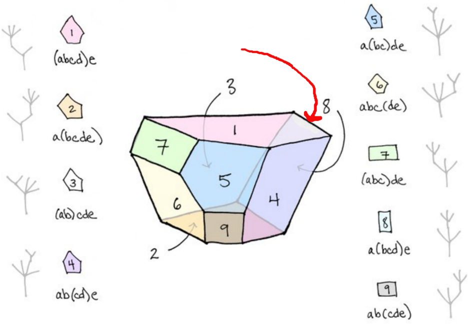
# Leaves as modulo classes

label each leaf of a tree by the modulo class to which it is mapped




The Fifth Associahedron $\mathcal{K}_5$

*(Diagram "borrowed" from Tai-Danae Bradley's* `www.math3ma.com` *blog.)*

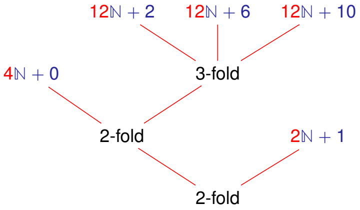



**An ordered exact, covering system** (P. Erdös, 1950s)

A sequence of <u>disjoint</u> modulo classes whose <u>union</u> is the whole of $\mathbb{N}$.

# The multiplicative coefficients

Multiplicative coefficients




In leaf-traversal ordering

$$4 = 2 \times 2$$

$$12 = 2 \times 2 \times 3$$

$$12 = 2 \times 2 \times 3$$

$$12 = 2 \times 2 \times 3$$

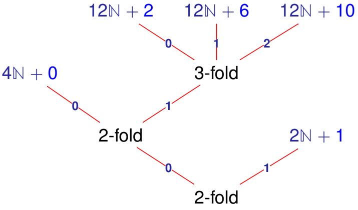
$$2 = 2 \ (!)$$

**To find multiplicative parts . . .**

Multiply the arities of each branching, from root to leaf.

# Counting paths

## Additive coefficients




## Path from leaf to root

$0 =$

| Base 2 | Base 2 |
|---|---|
| 0 | 0 |

$2 =$

| Base 3 | Base 2 | Base 2 |
|---|---|---|
| 0 | 1 | 0 |

$6 =$

| Base 3 | Base 2 | Base 2 |
|---|---|---|
| 1 | 1 | 0 |

$10 =$

| Base 3 | Base 2 | Base 2 |
|---|---|---|
| 2 | 1 | 0 |

$1 =$

| Base 2 |
|---|
| 1 |

### To find additive parts . . .

Write down the 'address' of each leaf[a]
& treat it as a number in a mixed-radix counting system
(with bases determined by the number of branchings).

[a] in **leaf-to-root** order!

A brief interlude

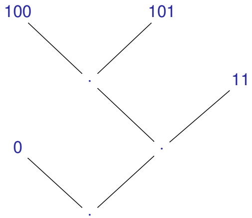
– a simple application –

# When all branchings have the same arity ...

**Well-known theory**

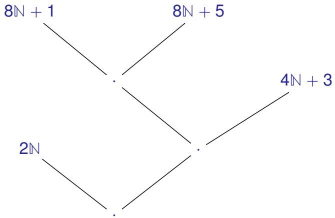
(Finite) trees with $k$-ary branchings are in 1:1 correspondence with (finite) maximal prefix codes over the free monoid $\{0, 1, \ldots, k-1\}^*$.

<u>root-to-leaf</u> paths




Maximal prefix code
$\{0, 100, 101, 11\} \subseteq \{0, 1\}^*$

<u>leaf-to-root</u> paths




Exact covering system
$\{2\mathbb{N}, 8\mathbb{N}+1, 8\mathbb{N}+5, 4\mathbb{N}+3\}$

# The general case

The set of **maximal prefix codes** over $\{0, \dots p-1\}^*$ is in 1:1 correspondence with exact covering systems whose multiplicative coefficients are of the form $p^x \in \mathbb{N}$.

Consider a (lexicographically ordered) maximal prefix code

$$\{w_0 \ , \ \dots \ , \ w_n\} \subseteq \{0, \dots, p-1\}^*$$

This uniquely determines an **exact covering system**

$$\left\{ p^{len(w_j)}\mathbb{N} + \|reverse(w_j)\|_{base\ p} \right\}_{j=0,1,\dots,n}$$

where :

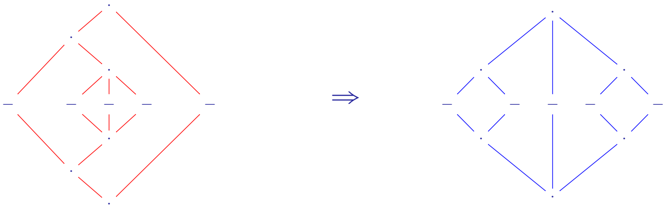
- $len : \{0, \dots, p-1\}^* \to (\mathbb{N}, +)$ is the **length homomorphism**.
- $reverse : \{0, \dots, p-1\}^* \to \{0, \dots, p-1\}^*$ is the **reversal anti-isomorphism**.
- $\| \_ \|_{base\ p} : \{0, \dots, p-1\}^* \to \mathbb{N}$ interprets a **string** as a (base-$p$) **number**.

End of interlude

– back to natural isomorphisms –

# Congruential functions as natural isomorphisms

Each of our composite conjunctions is based on an ordered covering system.



$\{4\mathbb{N}, 12\mathbb{N}+2, 12\mathbb{N}+6, 12\mathbb{N}+10, 2n+1\}$ $\{6\mathbb{N}, 6\mathbb{N}+3, 3\mathbb{N}+16\mathbb{N}+2, 6\mathbb{N}+4\}$

We build the canonical isomorphism between them by monotonically mapping between leaves :

| | | | |
|---|---|---|---|
| **leaf** 0 | $4\mathbb{N}$ | $\mapsto$ | $6\mathbb{N}$ |
| **leaf** 1 | $12\mathbb{N}+2$ | $\mapsto$ | $6\mathbb{N}+3$ |
| **leaf** 2 | $12\mathbb{N}+6$ | $\mapsto$ | $3\mathbb{N}+1$ |
| **leaf** 3 | $12\mathbb{N}+10$ | $\mapsto$ | $6\mathbb{N}+2$ |
| **leaf** 4 | $2\mathbb{N}+1$ | $\mapsto$ | $6\mathbb{N}+4$ |

# The general case

For arbitrary rooted planar trees, determining shuffles / generalised conjunctions :

| | | | |
|---|---|---|---|
| **leaf** $0$ | $A_0\mathbb{N} + B_0$ | $\mapsto$ | $C_0\mathbb{N} + D_0$ |
| **leaf** $1$ | $A_1\mathbb{N} + B_1$ | $\mapsto$ | $C_1\mathbb{N} + D_1$ |
| $\vdots$ | $\vdots$ | | $\vdots$ |
| **leaf** $n-1$ | $A_{n-1}\mathbb{N} + B_{n-1}$ | $\mapsto$ | $C_{n-1}\mathbb{N} + D_{n-1}$ |

The natural iso. between them has, as unique component, the bijection :

$$x \mapsto \frac{1}{A_j}\left(C_j x + \begin{vmatrix} A_j & B_j \\ C_j & D_j \end{vmatrix}\right) \text{ where } x \equiv B_j \mod A_j$$

# A general setting for natural isomorphisms

**Definition :** A function $f : \mathbb{N} \to \mathbb{N}$ is **congruential** if it is

*"defined piece-wise linearly on a family of modulo classes".*

More formally, there exists :

- An exact covering system $\{A_j\mathbb{N} + B_j\}_{j\in J}$
- A similarly-indexed family of rationals $\{(r_j, s_j)\}_{j\in J}$

such that

$$n \in A_j\mathbb{N} + B_j \quad \Rightarrow \quad f(n) = p_j n + q_j$$

**Motivated by problems of Lothar Collatz . . .**

**Theorem :** (J. Conway 1972)

Given

- A congruential function $f : \mathbb{N} \to \mathbb{N}$,
- A natural number $n \in \mathbb{N}$,

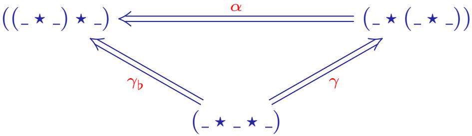
It is in general **undecidable** whether the orbit of $n$ under $f$ is **finite** or **infinite**.

# A disturbing possibility

**Questions :**

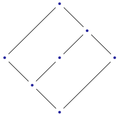
- Might we see *undecidable behaviour* from canonical isomorphisms ??
- If so, how *simple* might these be?

Let's make some natural isomorphisms explicit :

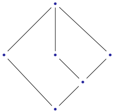


# Some ‘previously studied’ functions

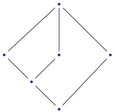
The **associator** *(Canonical associativity iso. for the conjunction of GoI I, II)*

$\alpha =$  giving $\alpha(n) = \begin{cases} 2n & n \equiv 0 \mod 2, \\ n+1 & n \equiv 1 \mod 4, \\ \frac{n-1}{2} & n \equiv 3 \mod 4. \end{cases}$

The **amusical permutation** *(Introduced by L. Collatz, named by J. Conway)*

$\gamma =$  giving $\gamma(n) = \begin{cases} \frac{2n}{3} & n \equiv 0 \mod 3, \\ \frac{4n-1}{3} & n \equiv 1 \mod 3, \\ \frac{4n+1}{3} & n \equiv 2 \mod 3. \end{cases}$

The **flattened permutation** (A ‘shifted’ version of the amusical permutation)

$\gamma_\flat =$  giving $\gamma_\flat(n) = \begin{cases} \frac{4n}{3} & n \equiv 0 \mod 3, \\ \frac{4n+2}{3} & n \equiv 1 \mod 3, \\ \frac{2n-1}{3} & n \equiv 2 \mod 3. \end{cases}$

satisfying $\gamma_\flat(n) + 1 = \gamma(n) + 1$

A couple more conjectures

# An unprovable(?) conjecture or two ...

**The Original Collatz Conjecture :** *Lothar Collatz (1932)*

The ‘amusical permutation’

$$\gamma(n) = \begin{cases} \frac{2n}{3} & n \equiv 0 \mod 3, \\ \frac{4n-1}{3} & n \equiv 1 \mod 3, \\ \frac{4n+1}{3} & n \equiv 2 \mod 3. \end{cases}$$

has infinite orbits – precisely, the orbit of 8 is infinite.

**Conway’s Unprovable Conjecture :** *J. Conway (2012)*

The *Original Collatz Conjecture* is the simplest possible example of an *undecidable arithmetic statement*.

Conway claimed the O.C.C. as the motivation for his proof of

undecidability in elementary arithmetic.

## Another application :

Thompson's $\mathcal{F}$, and the Original Collatz Conjecture

# Standard theory & interpretation (I)

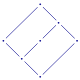
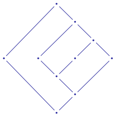
In the usual group-theoretic approach :

**Thompson's $\mathcal{F}$ is generated by two pairs of trees**


and


Interpreting as shuffles / deals (& hence canonical isomorphisms)) :

A subgroup of $\mathcal{S}(\mathbb{N})$ isomorphic to $\mathcal{F}$ is generated by

$\{ \alpha =$  $, \; Id \star \alpha =$  $\}$

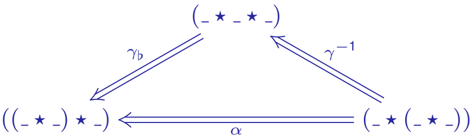
peter.hines@york.ac.uk 01232 457964

# Standard theory & interpretation (II)

Explicitly, $\mathcal{F}$ is generated by the congruential functions :

$$\alpha(n) = \begin{cases} 2n & n \equiv 0 \mod 2, \\ n+1 & n \equiv 1 \mod 4, \\ \frac{n-1}{2} & n \equiv 3 \mod 4. \end{cases} \quad , \quad (Id \star \alpha)(n) = \begin{cases} n & n \equiv 0 \ (mod\ 2) \\ 2n-1 & n \equiv 1 \ (mod\ 4) \\ n+2 & n \equiv 3 \ (mod\ 8) \\ \frac{n-1}{2} & n \equiv 7 \ (mod\ 8) \end{cases}$$

**Recall :** *Associativity* decomposes into *deleting brackets*, and *re-inserting brackets* :




peter.hines@york.ac.uk 01232 457964

# An (easily checkable) corollary . . .

As a corollary, Thompson's $\mathcal{F}$ is generated by the bijections

- $\alpha(n) \;=\; \gamma(\gamma^{-1}(n)+1)-1$
- $(Id \star \alpha)(n) \;=\; \begin{cases} n & n \text{ even,} \\ 2\gamma\left(\gamma^{-1}\left(\frac{n-1}{2}\right)+1\right)-1 & n \text{ odd.} \end{cases}$

This can be checked by elementary (albeit tedious . . . ) arithmetic calculations.

A couple more conjectures

# Two groups & a conjecture

Consider two subgroups of bijections $\mathcal{F} \subseteq \mathcal{C}_{\mathfrak{z}} \subseteq \mathcal{S}(\mathbb{N})$.

- $\mathcal{C}_{\mathfrak{z}}$ is generated by

$$\{\gamma \ , \ \gamma_\flat \ , \ \mathit{Id} \star \gamma \ , \ \mathit{Id} \star \gamma_\flat\}$$

- $\mathcal{F}$ is generated by

$$\{\alpha \ , \ \mathit{Id} \star \alpha\} \quad = \quad \{\gamma_\flat \gamma^{-1} \ , \ \mathit{Id} \star \gamma_\flat \gamma^{-1}\}$$

**Conjecture(s)**

1. It is *easy* to characterise orbits of natural numbers under members of $\mathcal{F}$.

   They are either **infinite** or **fixed points**.

2. $\mathcal{F}$ is precisely the subgroup of $\mathcal{C}_{\mathfrak{z}}$ consisting of bijections satisfying this property.

# References & Acknowledgements

https://arXiv.org/abs/2202.04443v1 From a conjecture of Collatz to Thompson's group $\mathcal{F}$, via a conjunction of Girard.

https://arxiv.org/abs/2206.07412v2 The inverse semigroup theory of elementary arithmetic.


Many thanks to :

**Matt Brin** (Binghampton), for history, theory, & references on Thompson groups & their connection with coherence.

**Jeffrey Lagarias** (Michigan), for references and anecdotes concerning Collatz's conjectures.

**Noson Yanofsky** (New York), for many in-depth discussions, leading to the development of this theory.

**Phil Scott** (In Memory), *For Everything . . .*