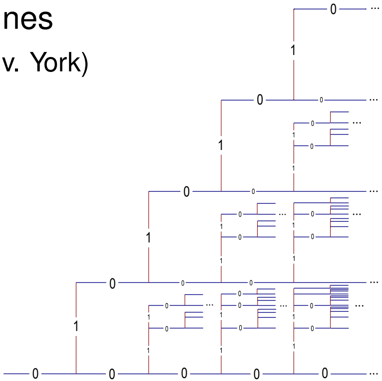
Shuffles, Operads, and Associahedra

Peter M. Hines
(Y.C.C.S.A. , Univ. York)

York Semigroup series

May – 2021



A simple starting point

Alice and Bob play a game against a dealer, with a countably infinite deck of cards.

The game is based around shuffling and dealing packs of cards.

- Fair deals (from the bottom of the pack).
- Perfect riffle shuffles.

The nature of my game

The Dealer deals out his (countably infinite) pack of cards, resulting in everyone holding an infinite stack of cards.

- Alice and Bob merge their stacks together, using a perfect riffle shuffle.
- The Dealer merges the result of this with his stack, again using a perfect riffle.

The process repeats. Each round of the game permutes the infinite pack of cards

Alice and Bob will win when

one card, that they mark <u>beforehand</u>,

returns to its original position

in the Dealer's hand.

The trap :

Alice and Bob are compulsive gamblers, who will not leave until they have won.

How to play the game?

This is not just a deterministic process.

In each round, Alice and Bob have a choice :

They can place the result of their shuffle to the **left** or the **right** of the Dealer's stack.

It then becomes the **first** or **second** deck in the Dealer's shuffle.

Strategies for Alice and Bob are strings over the set $\{0, 1\}$.

We should think of these as either in terms of

- Words over the free monoid $\{0, 1\}^*$
- Points of (binary) Cantor space $\mathfrak{C}$.

Exercise : For each choice of card $n \in \mathbb{N}$, characterise the subset $\mathfrak{U}_n \subseteq \mathfrak{C}$ of Cantor space where Alice & Bob are playing forever.

Does $\mathfrak{U}_n$ contain any open subsets, or do Alice and Bob always have a route to success?

The two paths you can go by ...

The left hand path Their result becomes the *first* deck in the Dealer's shuffle.

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

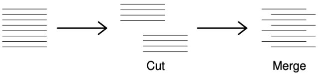
The right hand path Their result becomes the *second* deck in the Dealer's shuffle.

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

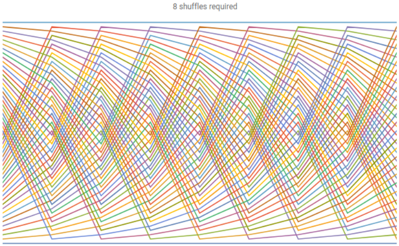
Which card should they mark ??

Alice and Bob, *for entirely unjustified reasons*, chose 8 as their 'lucky number'. They are more used to playing with 52 cards, where Riffle shuffles are performed by a *cut*,

then a *merge* :



A 52 card pack returns to its original position after 8 steps :



What happens in the countably infinite case?

A potentially poor strategy

When Alice and Bob consistently place their cards on the right :

The $3x+1$ **problem & its generalisations** – Jeffrey Lagarias (1985)

Writing about L. Collatz : *"In his notebook dated July 1, 1932, he considered the function*

$$n \mapsto \begin{cases} \frac{2}{3}n & \text{if } n \equiv 0 \ (mod\ 3) \\ \frac{4}{3}n - \frac{1}{3} & \text{if } n \equiv 1 \ (mod\ 3) \\ \frac{4}{3}n + \frac{1}{3} & \text{if } n \equiv 2 \ (mod\ 3) \end{cases}$$

He posed the problem of whether the cycle containing 8 *is finite or infinite. I will call this the* **Original Collatz Problem**. *His original question has never been answered."*

It is *conjectured*, and *widely believed*, that the cycle containing 8 is infinite.

It is entirely possible that the OCP is undecidable.
— if this is the case, we could never know.

(Almost) Lost Mathematics?

The **original Collatz problem** almost vanished into obscurity. It was *rescued* and *popularised* by Jeffrey Lagarias[1], who archives all things Collatz-related.

Unfortunately ..

We no longer have the original (1984) letter from Collatz to Lagarias describing his motivation :

- Why he was looking at this particular function?
- What is special about the number 8?
- Whether there is a connection to his (much) more famous problem??

Any story about Alice, Bob, and decks of cards is a *convenient fabrication* that nevertheless allows us to place this problem in context.

[1] Many thanks to J. Lagarias (Univ. Michigan), for useful references & anecdotes!

Providing context

Our overall claims :

- Alice & Bob's game should be thought of as 'tracing paths through geometric / combinatorial polyhedra'.
- There are many close connections with multiple topics in pure mathematics, logic, theoretical & practical computer science, and category theory.
- The (left- and right-) **Collatz bijections**

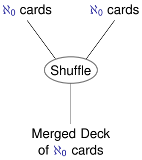
  $$\gamma_L : \mathbb{N} \rightarrow \mathbb{N} \quad \text{and} \quad \gamma_R : \mathbb{N} \rightarrow \mathbb{N}$$

  play a particularly important rôle in all these areas.
- These Collatz bijections are *canonical coherence isomorphisms*, in the sense of category theory.
- There is a close link between the original Collatz conjecture, and his more famous $3x + 1$ problem.

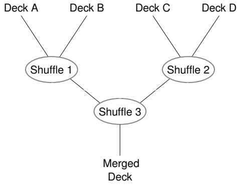
Splitting the game into individual steps

We wish to model (and compose) :

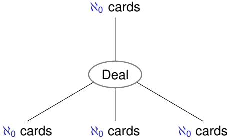
1. Shuffles of countably infinite Decks of Cards



2. Using the result of a shuffle as the input to another :



3. Deals, as an inverse operation to shuffles.



First – modeling infinitary shuffles

A (mathematical) strategy :

We simply take the (well-studied) finite case, and, “check everything still works”.

Shuffles are modeled by **monotone bijections**; bijectivity ensures all cards are used, and monotonicity accounts for,

“If card a is above card b before the shuffle,it is still above b afterwards.”

We axiomatise ‘multiple decks’ using the disjoint union, $\mathbb{N} \uplus \mathbb{N} = \mathbb{N} \times \{0\} \cup \mathbb{N} \times \{1\}$, and use the induced partial order :

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

Our shuffles are then (monotone) Hilbert-Hotel style bijections, and a **deal** is simply the inverse of a shuffle.

Starting to axiomatise ..

We define $\mathbf{Bij}_{\aleph_0}$ to be the groupoid given by :

Objects All *countably infinite sets*,

Arrows *Bijections* between c.i. sets.

Disjoint union defines a groupoid homomorphism $\_ \uplus \_ : \mathbf{Bij}_{\aleph_0} \times \mathbf{Bij}_{\aleph_0} \rightarrow \mathbf{Bij}_{\aleph_0}$.

A categorical tensor

This is a *semi-monoidal* tensor, satisfying all the usual MacLane-Kelly axioms, apart from those that mention a unit object.

Such structures were axiomatised and studied in

J. Kock (2008) *Elementary remarks on units in monoidal categories*

A. Joyal, J. Kock (2013) *Coherence for weak units*

We may therefore assume it is *strict*, so

$$X_0 \uplus X_1 \uplus \ldots \uplus X_k \overset{def.}{=} X_0 \times \{0\} \cup X_1 \times \{1\} \cup \ldots \cup X_k \times \{k\}$$

Shuffles as Cantor points

In both the finite & infinite case, we may describe a shuffle of k decks of cards as a *sequence* $p_0, p_1, p_2, p_3, \ldots$ over the set $\{0, \ldots, k-1\}$.

This has the intuition of an operational description :

"Take from deck p_0, then p_1, then p_2, then ..."

We recover this description by using the identity $\mathbb{N}^{\uplus k} \cong \mathbb{N} \times \{0, \ldots, k-1\}$,

$$\begin{tikzcd}
\mathbb{N} \arrow[rr, "\psi^{-1}"] \arrow[drr, "sequence_\psi"'] & & \mathbb{N} \times \{0, \ldots k-1\} \arrow[d, "\pi_2"] \\
& & \{0, \ldots, k-1\}
\end{tikzcd}$$

This point of the Cantor space over $\{0, \ldots, k-1\}$ is the **sequence of plays** for Ψ.

The two descriptions are entirely interchangeable – we will generally describe shuffles as *bijections*.

The riffle shuffles

We define the k-deck **riffle shuffle** $\Omega_k : \mathbb{N}^{\uplus k} \to \mathbb{N}$ to be the bijection $\Omega_k(n,i) = kn + i$ for all $(n,i) \in \mathbb{N}^{\uplus k}$, with the natural diagrammatics :

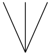
$\Omega_1 : \quad \mathbb{N} \to \mathbb{N}$

$n \mapsto n$

$\Omega_2 : \quad \mathbb{N} \uplus \mathbb{N} \to \mathbb{N}$

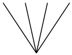
$(n,0) \mapsto 2n$
$(n,1) \mapsto 2n+1$

$\Omega_3 : \quad \mathbb{N} \uplus \mathbb{N} \uplus \mathbb{N} \to \mathbb{N}$



$(n,0) \mapsto 3n$
$(n,1) \mapsto 3n+1$
$(n,2) \mapsto 3n+2$

$\Omega_4 : \quad \mathbb{N} \uplus \mathbb{N} \uplus \mathbb{N} \uplus \mathbb{N} \to \mathbb{N}$

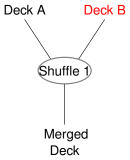


$(n,0) \mapsto 4n$
$(n,1) \mapsto 4n+1$
$(n,2) \mapsto 4n+2$
$(n,3) \mapsto 4n+3$

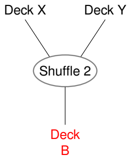
The inverse of Ω_n is the n-player **fair deal**.

Composition of shuffles

We wish to model **hierarchical composition** of shuffles, where we 'use the result of one shuffle as an input to another', and the **algebra** of how these may be composed.



where Deck B arises from



The natural setting for this is the theory of Operads

First, some intuition

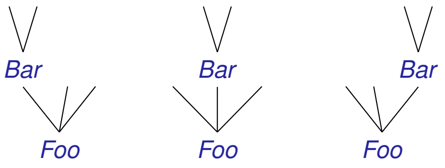
Consider 3-argument and 2-argument functions $Foo(\_,\_,\_)$ and $Bar(\_,\_)$ that accept, and return, elements of the same type[2].

There are three distinct ways to plug Bar into Foo to make an operation of arity 4.

$$Foo(Bar(\_,\_),\_,\_) \quad \text{or} \quad Foo(\_,Bar(\_,\_),\_) \quad \text{or} \quad Foo(\_,\_,Bar(\_,\_))$$

These are axiomatised as 'indexed compositions'.

$$Foo \circ_1 Bar \qquad Foo \circ_2 Bar \qquad Foo \circ_3 Bar$$



[2] Allowing for distinct data-types leads to the theory of 'coloured operads'.

A formal definition :

A (non-symmetric) **operad** consists of disjoint indexed sets of **operations**

$$\mathcal{H} = \{\mathcal{H}_1 , \mathcal{H}_2 , \mathcal{H}_3 , \ldots , \mathcal{H}_n , \ldots\}$$

– the *unary*, *binary*, *ternary*, , . . . , n-*ary* , . . . operations, which may be composed. Given

- an operation $F \in \mathcal{H}_x$,
- an operation $G \in \mathcal{H}_y$,

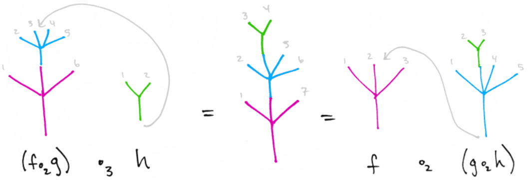
there are x different **compositions**

$$F \circ_1 G \ , \ F \circ_2 G \ , \ F \circ_3 G \ , \ \ldots \ , \ F \circ_x G$$

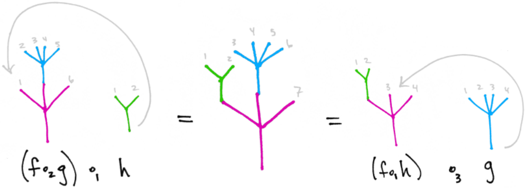
all giving an operation of arity $x + y - 1$.

Three simple axioms *(axiomatising Referential Transparency?)*

1. There exists an identity $Id \circ_1 T = T$ and $T \circ_k Id = T$.
2. "Composition is associative"



3. "Parallel composites commute"



Diagrams 'borrowed' from Tai-Danae Bradley's Math3ma blog

Formal definitions

An operad is an indexed family of disjoint sets $\mathcal{H} = \{\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3 \ldots\}$ of 'operations', together with composition functions

$$\circ_i : \mathcal{H}_n \times \mathcal{H}_m \rightarrow \mathcal{H}_{m+n-1} \quad , \quad i = 1 \ldots n$$

that include an identity in $\mathcal{H}_1$, and satisfy the following:

For all $f \in \mathcal{H}_n$, $g \in \mathcal{H}_m$, and $h \in \mathcal{H}_p$,

$$(f \circ_j g) \circ_i h = \begin{cases} (f \circ_i h) \circ_{j+p-1} g & \text{if } 1 \leqslant i \leqslant j-1 \\ f \circ_j (g \circ_{i-j+1} h) & \text{if } j \leqslant i \leqslant m+j-1 \\ (f \circ_{i-m+1} h) \circ_j g & \text{if } i \geqslant m+j \end{cases}$$

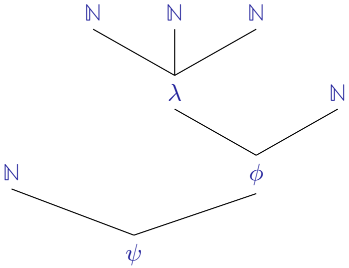
It is nearly always more convenient to work graphically!

Operads of card shuffles

Unsurprisingly, plugging together card shuffles forms an operad.

(It is an example of a standard construction :
the endomorphism operad in a semi-monoidal category)

A tree such as :



represents a shuffle (i.e. monotone bijection) of five decks of cards :

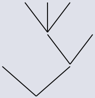
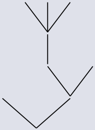
$$\psi(1_{\mathbb{N}} \uplus \phi(\lambda \uplus 1_{\mathbb{N}})) \ : \ \mathbb{N} \uplus \mathbb{N} \uplus \mathbb{N} \uplus \mathbb{N} \uplus \mathbb{N} \ \rightarrow \ \mathbb{N}$$

The object of study

We define $\mathcal{R}iff$, the operad of **hierarchical riffle shuffles** to be the operad generated by the perfect riffle shuffles $\{\Omega_k\}_{k>1}$

The obvious diagrammatics :

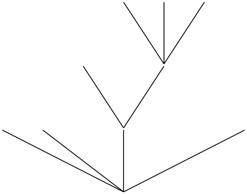
- As we only have one generator of each arity, we may draw H-R shuffles as *unlabled planar trees*.
- We leave identities implicit.

We do not distinguish between  and 

Each k-leaf tree determines a monotone Hilbert-hotel style bijection from k copies of $\mathbb{N}$ to a single copy of $\mathbb{N}$.

What bijections do they determine??

An illustrative example : $\mathcal{T} \;=\; \Omega_4 \circ_3 (\Omega_2 \circ_2 \Omega_3) \;=\; (\Omega_4 \circ_3 \Omega_2) \circ_4 \Omega_3$



$$\mathcal{T}(n,i) = \begin{cases} 4n & i = 0 \\ 4n+1 & i = 1 \\ 8n+2 & i = 2 \\ 24n+6 & i = 3 \\ 24n+14 & i = 4 \\ 24n+22 & i = 5 \\ 4n+3 & i = 6 \end{cases}$$

Each $\mathcal{T}(\_, i)$ is a linear map $n \mapsto X_i n + Y_i$.

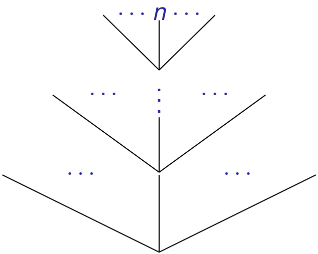
As $\mathcal{T}$ is a **bijection**,

$$im(\mathcal{T}(\_, i)) \;\cap\; im(\mathcal{T}(\_, j)) \;=\; \varnothing \quad \text{and} \quad \bigcup_{i=0}^{7} im(\mathcal{T}(\_, j)) \;=\; \mathbb{N}$$

The bijection $\mathcal{T}$ *'covers the natural numbers with linear sequences'*.

Counting coefficients

The general case, card n from deck i :



Branch a_k out of b_k

$\cdots$

Branch a_2 out of b_2

Branch a_1 out of b_1

We have an injection $n \mapsto X_i n + Y_i$. How to compute X_i and Y_i ?

- Trivially, $X_i = \prod_{j=1}^{k} b_j$.

  (Corollary : we cannot have $X_i = X_j \ \forall i, j$, for a prime number of decks of cards).

- We may simply <u>write down</u> the value of Y_i.

Relating two strands of Cantor's work

Über Einfache Zahlensysteme" – G. Cantor (1869)

On Simple Number Systems studied **mixed-radix** counting : positional number systems where the *base* used varies between *columns*.

Familiar example : pre-decimal / post-brexit British currency

4 Farthings = 1 Penny , 12 Pennies = 1 Shilling , 20 Shillings = 1 Pound ...

We may simply write down the value of Y_i

$Y_i =$

base b_k	base b_{k-1}	$\dots$	base b_1
a_k	a_{k-1}	$\dots$	a_1

(Note : $b_k b_{k-1} \dots b_1$ is an ordered factorisation of X_i).

Transformations between different mixed-radix counting systems are particularly well-studied in the Fast Fourier Transforms re-discovered by Cooley & Tukey (... but originally due to Gauss).

Topological connections

It is natural to interpret Shuffles as determining open covers of $\mathbb{N}$.

Recall : Every shuffle $T \in \mathcal{R}iff_k$ determines a distinct[3] indexed family $\{T(\_, i) : \mathbb{N} \to \mathbb{N}\}_{i=0..k-1}$ of linear maps.

Their images satisfy, for all $i \neq j$,

$$T(\mathbb{N}, i) \ \cap \ T(\mathbb{N}, j) \ = \varnothing \quad , \quad \bigcup_{i=0}^{k-1} T(\mathbb{N}, i) \ = \ \mathbb{N}$$

and so “cover” the natural numbers with disjoint linear sequences.

This should be thought of topologically — every shuffle determines a (distinct) ordered *finite open cover* of $\mathbb{N}$, in some suitable topology.

---

[3] Claim to be justified shortly ...

From topologies to primes

Define the **linear subsets** of $\mathbb{N}$ by $lin = \{a\mathbb{N} + b\}_{b<a\in\mathbb{N}} \cup \{\varnothing\}$.

This contains $\mathbb{N}$ and $\{\varnothing\}$. By the *Chinese Remainder Theorem*, it is also closed under intersection.

It is therefore the basis for a topology $pro \subseteq 2^{\mathbb{N}}$, the **profinite topology** on the free monogenic monoid.

1. Introduced by Ch. Reutenauer, *Une topologie du monoïde libre* (1979)
2. Based on the profinite topology for groups (M. Hall 1950)
3. Also used by H. Furstenberg (1955), to give a topological proof of the infinitude of the primes.

Our interest : All the operations we will consider, including the Collatz bijections, will be continuous (in fact, homeomorphisms) w.r.t. this topology.

Some points on the profinite topology of $(\mathbb{N}, +)$

1. The basic open sets are **clopen** – both open and closed. We may write $a\mathbb{N} + b$ as the complement of the open set $\bigcup_{c \neq b} a\mathbb{N} + c$.

2. Open sets are always infinite (the key to Furstenberg's proof ...)

3. There is an isomorphism (of locales) between
   - The subtopology with basis $\{k^a\mathbb{N} + b\}_{b<k^a} \subseteq pro$.
   - The usual clopen topology on the k^{th} Cantor space $\mathfrak{C}_k$

     – i.e. the space of one-sided infinite strings over $\{0, \ldots, k-1\}$.

The correspondence

A basic open set of $\mathfrak{C}_k$ is of the form $w\mathfrak{C}_k$, for some word w of the free monoid $\{0, \ldots, k-1\}^*$.

Denote the length of w by $|w|$, then interpret w itself as a k-ary number.

The corresponding linear subset is $k^{|w|+1}\mathbb{N} + w$.

Remark These arise from the sub-operad of $\mathcal{R}iff$ generated by Ω_k.

To justify the claim of "uniqueness"

Proposition : $\mathcal{R}iff$ is *freely generated* by $\{\Omega_j\}_{j=2,3,4,\ldots}$.

No two distinct k-leaf trees determine the same bijection from $\mathbb{N}^{\uplus k}$ to $\mathbb{N}$.

i.e. $\mathcal{R}iff$ is isomorphic to the formal operad **rpt** of "rooted planar trees".

Proof (outline) : This may be shown by induction on the number of leaves.

The only non-trivial step

We need to show that the generating set $\{\Omega_K\}_{k>0}$ is *minimal* — no perfect riffle can be produced by composing other perfect riffles.

We do this by showing that the generators Ω_K are a very special type of shuffle.

Definition A shuffle of k decks of cards $\Psi : \mathbb{N} \times \{0, \ldots, k-1\} \to \mathbb{N}$ is **standard** when it is **monotone in both variables**.

Standard shuffles

An operational characterisation :

This has the natural interpretation that, at any stage of the shuffle,

$$\#\text{ of cards placed from deck } i \geqslant \#\text{ of cards placed from deck } i+1$$

As a consequence, the sequence of plays will be an infinitary Ballot sequence.

Equivalently : The tableau determined by a standard shuffle is a (infinitary) standard Young tableau, with ordered rows & columns.

$\Psi(0,0)$	$\Psi(1,0)$	$\Psi(2,0)$	$\Psi(3,0)$	$\dots$
$\Psi(0,1)$	$\Psi(1,1)$	$\Psi(2,1)$	$\Psi(3,1)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$\Psi(0,k-1)$	$\Psi(1,k-1)$	$\Psi(2,k-1)$	$\Psi(3,k-1)$	$\dots$

The generators $\{\Omega_1, \Omega_2, \Omega_3, \dots\}$ are certainly standard – which composites are similarly standard?

Characterising standard riffle shuffles

For a composite $S \circ_k T$ to be standard, we need the following :

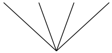
1. S and T are themselves both standard.
2. S is of arity k – i.e. the product is the (associative) **overproduct**

$$S \urcorner T \stackrel{def.}{=} S \circ_k T \quad \forall S \in \mathcal{R}iff_k$$

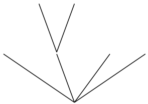
given by **grafting onto the far right leaf**.

As an illustrative example, consider $\Omega_4 \circ_2 \Omega_2$. All the generators are standard, but this composite is not standard :

0	4	8	12	16	...
1	5	9	13	17	...
2	6	10	14	18	...
3	7	11	15	19	...



0	4	8	12	16	...
1	9	17	25	33	...
5	13	21	29	36	...
2	6	10	14	18	...
3	7	11	15	19	...



Operadic composition as ‘splitting rows’

In the general setting, consider some standard $\Psi \in \mathcal{R}iff_k$, with tableau

$\Psi(0,0)$	$\Psi(1,0)$	$\Psi(2,0)$	$\Psi(3,0)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$\Psi(0,x)$	$\Psi(1,x)$	$\Psi(2,x)$	$\Psi(3,x)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$\Psi(0,k-1)$	$\Psi(1,k-1)$	$\Psi(2,k-1)$	$\Psi(3,k-1)$	$\dots$

For some standard $\Phi \in \mathcal{R}iff_j$, the tableau for $\Psi \circ_x \Phi$ is given by replacing row x by the following block :

$\Psi(0,0)$	$\Psi(1,0)$	$\Psi(2,0)$	$\Psi(3,0)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$\Psi(\Phi(0,0),x)$	$\Psi(\Phi(1,0),x)$	$\Psi(\Phi(2,0),x)$	$\Psi(\Phi(3,0),x)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$\Psi(\Phi(0,j-1),x)$	$\Psi(\Phi(1,j-1),x)$	$\Psi(\Phi(2,j-1),x)$	$\Psi(\Phi(3,j-1),x)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$\Psi(0,k-1)$	$\Psi(1,k-1)$	$\Psi(2,k-1)$	$\Psi(3,k-1)$	$\dots$

The ‘standard’ property is preserved precisely when the final row is split.

Standard $\equiv$ Right-Associated

We may characterise standard hierarchical riffle shuffles

These are given by arbitrary overproducts of generators.

$$\Omega_{x_0} \urcorner\!\!\downarrow \Omega_{x_1} \urcorner\!\!\downarrow \Omega_{x_2} \urcorner\!\!\downarrow \ldots \urcorner\!\!\downarrow \Omega_{x_N}$$

No generator is a non-trivial composite of this form; therefore, the generating set is minimal, and by induction $\mathcal{R}iff$ is freely generated.

Every distinct finite sequence of natural numbers determines a distinct standard shuffle / standard Young tableau, by

$$n_0 n_1 \ldots n_x \;\mapsto\; \Omega_{n_0+2} \urcorner\!\!\downarrow \Omega_{n_1+2} \urcorner\!\!\downarrow \ldots \urcorner\!\!\downarrow \Omega_{n_x+2}$$

i.e. there exists an injective monoid homomorphism from the free monoid over the natural numbers to $(\mathcal{R}iff, \urcorner\!\!\downarrow)$, given by $std(n) \stackrel{def}{=} \Omega_{n+2}$.

A brief digression ...

Operads with infinitary compositions?

From monoids to Cantor spaces

We may extend this to *one-sided infinite* strings (i.e. points of $\mathfrak{C}_{\mathbb{N}}$, the Cantor space over the natural numbers) in a natural way.

Consider some infinite sequence

$$\Omega_{x_0} \linefeed \Omega_{x_1} \linefeed \Omega_{x_2} \linefeed \Omega_{x_3} \linefeed \ldots$$

along with the sequence of tableaux determined by the prefixes :

1. Ω_{x_0}
2. $\Omega_{x_0} \linefeed \Omega_{x_1}$
3. $\Omega_{x_0} \linefeed \Omega_{x_1} \linefeed \Omega_{x_2}$
4. $\Omega_{x_0} \linefeed \Omega_{x_1} \linefeed \Omega_{x_2} \linefeed \Omega_{x_3}$

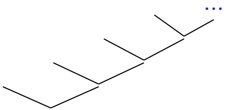
At each step, every natural number N either:

- moves left (& possibly downwards as well), or
- stays in the same place ... at which point it remains there!

These will define *infinitary standard shuffles*, or monotone bijections $\mathbb{N} \times \mathbb{N} \cong \mathbb{N}$.

The simplest worked example:

The simplest is the infinitary overproduct $\Omega_2 ↴ \Omega_2 ↴ \Omega_2 ↴ \Omega_2 ↴ \ldots$ that may be thought of as "the right fixed point for the binary riffle shuffle" :



We may give this explicitly, as the **"of course" bijection**

$$!(x, y) \; = \; 2^{x+1}y + 2^x - 1$$

a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$, monotone in *both* variables.

Why 'of course' ?

I first came across this function being used to model a logical operation (the "exponential", a.k.a. the "bang" or "of course" modality) in :

"Geometry of Interaction (I) : interpretation of System $\mathcal{F}$"

– Jean-Yves Girard (1989)

.

Shuffling infinitely many decks of cards ..

Giving the tableau explicitly :

0	2	4	6	8	10	...
1	5	9	13	17	21	...
3	11	19	27	35	43	...
7	23	39	55	71	87	...
15	47	79	111	143	175	...
31	94	159	223	287	351	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

The sub-tableaux given by considering the first n natural numbers

form an inclusion-ordered unbounded sequence of

finitary standard Young tableaux,

for **any** monotone bijection

$$\Psi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

Shuffling infinitely many decks of cards ??

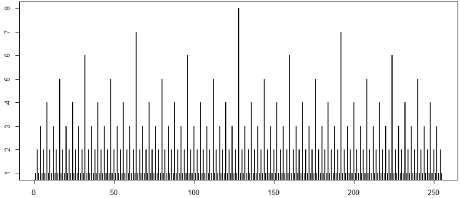
Alternatively, the **sequence of plays** $\pi_2!^{-1} : \mathbb{N} \to \mathbb{N}$ is given by

0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 4 0 1

0 2 0 1 0 3 0 1 0 2 0 1 0 5 0 1 0 2

0 1 0 3 0 1 0 2 0 ...

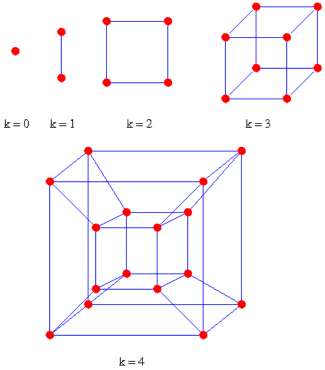
This is the (ballot) **ruler sequence** — sequence number A007814 in the Online Encyclopedia of Integer Sequences (`https://oeis.org/A007814`)



Picture taken from "On the ubiquity of the Ruler sequence" – J. Nuño, F. Muñoz (2020)

A fun application

The ruler sequence $r(n)$ determines Hamiltonian paths (– those that visit each vertex exactly once) in hypercube graphs :



The simple prescription :

- Index axes (i.e. dimensions) by the natural numbers,
- On step n, move along axis $r(n)$.

visits each vertex exactly once.

Concretely, *how could we perform this shuffle??*

The ruler series is the sequence of plays for the bijection ! $=$ Ω_2 ↴ Ω_2 ↴ Ω_2 ↴ Ω_2 ↴ . . .

				1	**0**
			1	0	**1**
			1	1	**0**
		1	0	0	**2**
		1	0	1	**0**
		1	1	0	**1**
		1	1	1	**0**
	1	0	0	0	**3**
	1	0	0	1	**0**
	1	0	1	0	**1**
	1	0	1	1	**0**
	1	1	0	0	**2**
	1	1	0	1	**0**
	1	1	1	0	**1**
	1	1	1	1	**0**
1	0	0	0	0	**4**

For an arbitrary (infinite) overproduct Ω_{x_0} ↴ Ω_{x_1} ↴ Ω_{x_2} ↴ Ω_{x_3} ↴ . . ., we simply count in a mixed-radix system with columns labeled by $\ldots, x_3, x_2, x_1, x_0$.

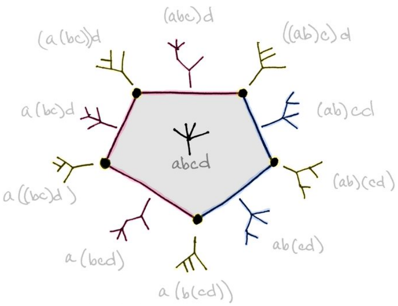
Back to the finite setting ...

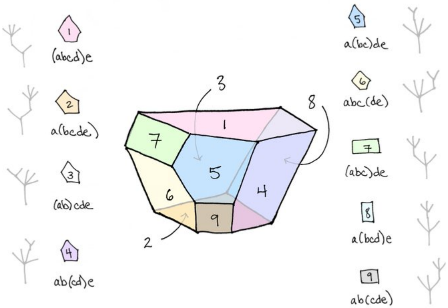
We now consider combining Shuffles and Deals

and recover the setting for Alice & Bob's game.

Associahedra and Shuffles

The operad **rpt** of Rooted Planar Trees ($\cong \mathcal{R}iff$) has a (very) close connection with the **associahedra** introduced by J. Stasheff in his PhD thesis (see also D. Tamari, S. MacLane, J. Milnor).





Diagrams again 'borrowed' from T.-D. Bradley's blog, **www.math3ma.com**.

Our interpretation

The facets (vertices, edges, faces, etc.) of the associahedron $\mathcal{K}_n$ are simply n-leaf rooted planar trees, or well-bracketed strings of symbols.

Mappings between facets arise as composites of *deleting* and *inserting* pairs of brackets

In our setting ...

We interpret

"facets of $\mathcal{K}_n$" as "shuffles of n decks of cards"

which leads to

"mappings between facets" as "bijections on the natural numbers".

We derive bijections on the natural numbers that,

"rearrange the result of one shuffle into that of another",

and consider these to live within $\mathcal{I}_{\mathbb{N}}$, the symmetric inverse monoid.

Mappings between shuffles / facets?

Give $\Phi, \Psi \in \mathcal{R}iff_k$, re-arranging the result of Φ into that of Ψ is performed by a bijection on $\mathbb{N}$

$$\begin{tikzcd} & \mathbb{N} \uplus \ldots \uplus \mathbb{N} \arrow[dl, "\Psi"'] \arrow[dr, "\Phi"] & \\ \mathbb{N} & & \mathbb{N} \arrow[ll, "\Psi\Phi^{-1}"] \end{tikzcd}$$

A definition

We define the k**-deck rearrangements**

$$\mathcal{R}_1 \hookrightarrow \mathcal{R}_2 \hookrightarrow \mathcal{R}_3 \hookrightarrow \mathcal{R}_4 \hookrightarrow \ldots$$

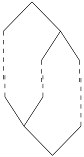
to be the inclusion-ordered sequence of sets of bijections given by :

$$\mathcal{R}_k \ = \ \{\Psi\Phi^{-1} \ : \Psi, \Phi \in \mathcal{R}iff_k\} \ \subseteq \ \mathcal{I}_{\mathbb{N}}$$

giving the **rearrangements** as their union, $\mathcal{R} = \bigcup_{j=1}^{\infty} \mathcal{R}_j$.

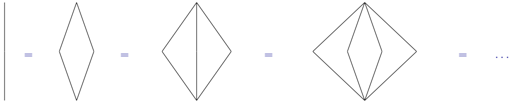
Diagrammatics and sequences

We use the obvious diagrammatic notation for composites of

of shuffles & inverses of shuffles, such as : 

The *inclusion-ordering* $\mathcal{R}_1 \hookrightarrow \mathcal{R}_2 \hookrightarrow \mathcal{R}_3 \hookrightarrow \ldots$ then comes from

the identities $Id_{\mathbb{N}} = \Omega_2{\Omega_2}^{-1} = \Omega_3\Omega_3^{-1} = \Omega_4\Omega_4^{-1} = \ldots$

which may be drawn as : 

In general, for all $S, T \in Riff_k$, and $X \in \mathcal{R}iff_N$

$$(S \circ_r X)(T \circ_r X)^{-1} = ST^{-1} \in \mathcal{I}_{\mathbb{N}}$$

Rearrangements in context

Each rearrangement is a (finite, disjoint) union of monotone partial injections :

$$\{a_i\mathbb{N} + b_i \ \mapsto \ c_i\mathbb{N} + d_i\}_{i=1\ldots K}$$

(with an obvious connection with Nivat & Perot's polycyclic monoids).

They are bijective versions of *congruential functions*, defined in

"Unpredictable Iterations" – J. Conway (1971)

used to encode Turing machine halting problems (undecidability / universal computability) on iterated functions systems such as Collatz's operators.

They are also a very special form of congruential function, used in

"Functional equations associated with congruential functions"
— S. Berckel (1994)

to simplify & extend Conway's result.

Historical question : Were Soviet mathematicians (e.g. S. Maslov / Y. Matiasevich) also aware of Conway's / Berckel's results ??

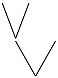
Some illustrative examples

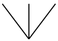
The simplest non-trivial example, $\mathcal{K}_3$, has two vertices, and one edge.

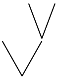
$$((\bullet\bullet)\bullet) \;\xrightarrow{\hspace{2em}} (\bullet\bullet\bullet) \xrightarrow{\hspace{2em}}\; (\bullet(\bullet\bullet))$$

Interpreted as card shuffles, we have

$Left = \Omega_2 \circ_1 \Omega_2$ $\qquad\qquad$ Ω_3 $\qquad\qquad$ $Right = \Omega_2 \circ_2 \Omega_2$





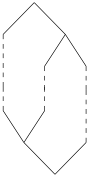


$$Left(n,i) = \begin{cases} 4n & i=0 \\ 4n+2 & i=1 \\ 2n+1 & i=2 \end{cases} \qquad \Omega_3(n,i) = \begin{cases} 3n & i=0 \\ 3n+1 & i=1 \\ 3n+2 & i=2 \end{cases} \qquad Right(n,i) = \begin{cases} 2n & i=0 \\ 4n+1 & i=1 \\ 4n+3 & i=2 \end{cases}$$

Mapping between three-deck shuffles

$$((\bullet\bullet)\bullet) \longleftarrow (\bullet\bullet\bullet) \longrightarrow (\bullet(\bullet\bullet))$$

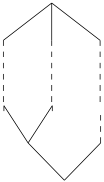
$\alpha \;=\; Left.Right^{-1}$



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

The **associator**

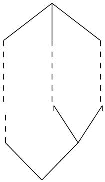
$\gamma_L \;=\; Left.\Omega_3^{-1}$



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

The **(left) Collatz bijection**

$\gamma_R \;=\; Right.\Omega_3^{-1}$



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

The **(right) Collatz bijection**

Alice and Bob split the associator

The associator α and its inverse α^{-1} factor in a natural way, as

$$\begin{tikzcd} \mathbb{N} & \mathbb{N} \arrow[l, "\gamma_L"'] & \mathbb{N} \arrow[l, "\gamma_R^{-1}"'] \arrow[ll, bend left, "\alpha"] \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} \mathbb{N} \arrow[r, "\gamma_L^{-1}"'] \arrow[rr, bend left, "\alpha^{-1}"] & \mathbb{N} \arrow[r, "\gamma_R"'] & \mathbb{N} \end{tikzcd}$$

where we may give γ_L^{-1} and γ_R^{-1} explicitly, as

$$\gamma_L^{-1}(n) = \begin{cases} \frac{3n}{4} & n \ (mod\ 4) = 0 \\ \frac{3n-2}{4} & n \ (mod\ 4) = 2 \\ \frac{3n+1}{2} & n \ (mod\ 2) = 1 \end{cases} \quad \text{and} \quad \gamma_R^{-1}(n) = \begin{cases} \frac{3n}{2} & n \ (mod\ 2) = 0 \\ \frac{3n+1}{4} & n \ (mod\ 4) = 1 \\ \frac{3n-1}{4} & n \ (mod\ 4) = 3 \end{cases}$$

About the associator α :

1. It is an *associativity isomorphism* from category theory.
2. It is central to some *logical models*.
3. It is core to some well-known *group theory*, *complexity theory*, and *cryptography*.

Elementary properties

For arbitrary rearrangments, we may write down some basic properties.

1. $\mathcal{R}_1 = \mathcal{R}_2 = \{Id_{\mathbb{N}}\}$.
2. $\mathcal{R}_k$ is closed under inverses : $(TS^{-1})^{-1} = (ST^{-1})$
3. $\mathcal{R}_k$ is not closed under the composition of $\mathcal{I}_{\mathbb{N}}$, for $k > 2$.
4. A family of composites that *are* contained in $\mathcal{R}_k$ is

   those of the form $(UT^{-1})\,(TS^{-1}) \;=\; (US^{-1})\;,\;\; S, T, U \in \mathcal{R}iff_k$
5. Each rearrangement is a homeomorphism w.r.t. the profinite topology.
6. There is a sequence of embeddings $R_1 \hookrightarrow R_2 \hookrightarrow R_3 \hookrightarrow R_4 \hookrightarrow R_5 \hookrightarrow \ldots$

A 'posetal' property

Point 4 is the triviality that, for any three k-deck shuffles S, T, U, the following diagram commutes :

$$
\begin{tikzcd}
\mathbb{N}^{\oplus k} \arrow[d, "U"'] & \mathbb{N}^{\oplus k} \arrow[l, "Id_{\mathbb{N}^{\oplus k}}"'] \arrow[d, bend left, "T"] & \mathbb{N}^{\oplus k} \arrow[l, "Id_{\mathbb{N}^{\oplus k}}"'] \\
\mathbb{N} & \mathbb{N} \arrow[l, "UT^{-1}"] \arrow[u, bend left, "T^{-1}"] & \mathbb{N} \arrow[l, "TS^{-1}"] \arrow[u, "S^{-1}"']
\end{tikzcd}
$$

However, recall the correspondence between shuffles and formal trees. We may also interpret this as a functor / groupoid homomorphism.

A definition

Let us denote by $\mathbb{RPT}$ the groupoid whose objects are rooted planar trees, where $\mathbb{RPT}(S, T)$ has a *single element* iff S, T have the same number of leaves, and is *empty* otherwise.

There is then an obvious functor from $\mathbb{RPT}$ to $\mathcal{I}_{\mathbb{N}}$.

The obvious functor

We define the functor / homomorphism $\Gamma : \mathbb{RPT} \to \mathcal{I}_{\mathbb{N}}$ as follows :

Objects $\Gamma(T) = \mathbb{N}$, for all trees $T \in Ob(\mathbb{RPT})$

Arrows Given k-leaf trees $S, T \in Ob(\mathbb{RPT})$, let us

- Denote the unique arrow of $\mathbb{RPT}(S, T)$ by $S \to T$
- Denote the interpretation of S, T as *shuffles* by $\ulcorner S \urcorner, \ulcorner T \urcorner : \mathbb{N}^{\uplus k} \to \mathbb{N}$.

Using this notation, $\Gamma(S \to T) = \ulcorner T \urcorner \ulcorner S \urcorner^{-1}$

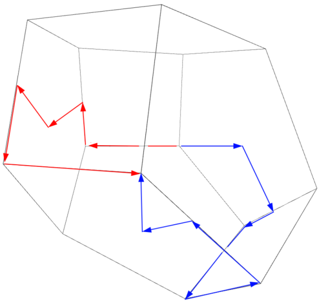
Functoriality follows rather trivially!

However, we may

1. interpret formal tree re-arrangements as bijections on the natural numbers,
2. build commuting diagrams, based on associahedra, over $\mathcal{I}_{\mathbb{N}}$.

Commuting diagrams ...

Arbitrary paths through $\mathcal{K}_n$ may be labeled by elements of $\mathcal{R}_n$.



The composite along any two paths *with the same source and target* is the same.

The sequence of inclusions $\mathcal{R}_1 \hookrightarrow \mathcal{R}_2 \hookrightarrow \mathcal{R}_3 \hookrightarrow \mathcal{R}_4 \hookrightarrow \ldots$ means that each path in $\mathcal{K}_n$ determines multiple paths in $\mathcal{K}_{n+a}$, with the same labels.

A question of emhpasis

The (Computer Science?) interpretation as congruential bijections is “untyped” — we consider paths between arbitrary facets of arbitrary associahedra.

This is in contrast to :

Algebra It is common to consider mappings defined by trees where all branchings have the same arity (binary trees, ternary trees, etc.)

The polycyclic monoids & Thompson groups revisited — M. V. Lawson (2020)

Category theory / coherence This studies mappings between trees with the same *geometric* interpretation (vertices, edges, faces, etc.)

A survey of definitions of n-categories — T. Leinster (2001)

Where algebra meets category theory meets logic ...

The algebraic and categorical approaches are **distinct**, except when considering 1-skeletons (vertices & edges) of associahedra – *mappings between binary trees*.

A relevant reference or two ...

Via two different routes, we arrive at the same place :

Category Theory A categorical characterisation of Thompson's group $\mathcal{F}$
– *M. Fiore, T. Leinster* (2010)

Algebra The Polycyclic Monoids & The Thompson Groups"
– *M. Lawson (2007)*

The key result ...

As a corollary of either of these, the congruential functions derived from the sub-operad of binary trees form a group : Richard Thompson's group $\mathcal{F}$.

These correspond to mappings between vertices of associahedra.

Questions :

1. Can we characterise (algebraically or categorically) mappings between *adjacent* vertices?
2. Can we express Thompson's $\mathcal{F}$ as a group generated by Collatz bijections?
3. What is the connection with category theory?

Time for a definition!

Abstractly, it may be defined as the group with:

- A countably infinite set of generators $\{x_0, x_1, x_2, \ldots\}$
- Relations given by
$$x_k^{-1} x_n x_k \;=\; x_{n+1} \quad \text{for all} \;\; k < n$$

Other presentations are possible, but this is the most **standard** (pun intended).

It also has a particularly relevant description as :

– *pairs of binary trees with the same number of leaves.*

which we naturally interpret as

– *pairs of vertices on the same associahedron.*

– *pairs of shuffles in the sub-operad of* $\mathcal{R}iff$ *generated by* Ω_2*.*

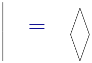
A graphical illustration

In, for example, José Burillo's book "Introduction to Thompson's group $\mathcal{F}$", we find the key notion of *equivalence* that accounts for both *deciding equality*, and *composition*.

- Given binary trees R, S, T, then composition satisfies $(T, S)(S, R) = (T, R)$.
- We should think of *equivalence classes* of trees

is equivalent to

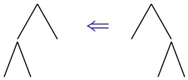
From our viewpoint ..

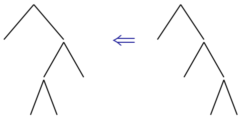
1. One of these pairs is upside down
2. They should be connected at the leaves.
3. The key 'eliminating matching carets' step  is the first in a series of identities giving inclusions of rearrangements

$$\mathcal{R}_1 \hookrightarrow \mathcal{R}_2 \hookrightarrow \mathcal{R}_3 \hookrightarrow \mathcal{R}_4 \hookrightarrow \ldots$$

Standard theory & explicit calculations ...

It is well-known (e.g. Burillo's book) that two pairs of trees are enough to generate the whole of $\mathcal{F}$





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

This is the associator α.

$$n \mapsto \begin{cases} n & n \ (mod\ 2) = 0 \\ 2n-1 & n \ (mod\ 4) = 1 \\ n+2 & n \ (mod\ 8) = 3 \\ \frac{n-1}{2} & n \ (mod\ 8) = 7 \end{cases}$$

How to describe this?

We need some category theory ...

It is by now folklore (i.e. rediscovered many times) that :

Given a (non-abelian) monoid with a categorical tensor, the associativity isomorphisms form an isomorphic copy of $\mathcal{F}$.

A **non-comprehensive** list :

- **R. McKenzie, R. Thompson** (1971): Close connection between Thompson's group $\mathcal{F}$, and associativity laws
- **PMH, M. V. Lawson** (1998) A class of associativity isomorphisms via inverse semigroup theory.
- **K. Brown** (2004) A group homomorphism $\_ \star \_ : \mathcal{F} \times \mathcal{F} \rightarrow \mathcal{F}$ that is *associative up to conjugation by some fixed element.*
- **P. Dehornoy** (2005) 'The only [non-trivial] relations in this presentation of $\mathcal{F}$ correspond to the well-known MacLane-Stasheff pentagon.'
- **M. Brinn** (2005) 'the resemblance of the usual coherence theorems with Thompson's group $\mathcal{F}$'.
- **M. V. Lawson** (2006) The associativity isomorphisms from inverse semigroup theory form a copy of $\mathcal{F}$.
- **M. Fiore, T. Leinster** (2010) Thompson's group $\mathcal{F}$ is the symmetry group of an idempotent U in the free strict monoidal category generated by U. (Equivalently, $\mathcal{F}$ is the *free semi-monoidal category* with one object).
- **PMH** (2016) "In the free case, this group [of asociators] is Thompson's $\mathcal{F}$."

What is the monoid / tensor associated with this description of $\mathcal{F}$ as congruential bijections ??

Shuffles in conjunction

In his *"Geometry of Interaction"* series of papers, Jean-Yves Girard gave representations of (various fragments of) Linear Logic, within $\mathcal{I}_{\mathbb{N}}$, the symmetric inverse monoid on the natural numbers.

Particularly relevant is the model of **conjunction** found in

"Geometry of Interaction (I) : interpretation of System $\mathcal{F}$" (1989)

Given partial injections $f, g \in \mathcal{I}_{\mathbb{N}}$, define $[f \star g](n) = \begin{cases} 2.f\left(\frac{n}{2}\right) & n \text{ even,} \\ 2.g\left(\frac{n-1}{2}\right)+1 & n \text{ odd.} \end{cases}$.

This is an injective homomorphism / categorical tensor

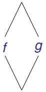
His 'conjunction' $[\_ \star \_] : \mathcal{I}_{\mathbb{N}} \times \mathcal{I}_{\mathbb{N}} \to \mathcal{I}_{\mathbb{N}}$ satisfies :

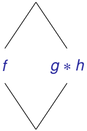
- $[f \star g][h \star k] = fh \star gk$.
- $[Id \star Id] = Id$
- $[f \star g]^{-1} = \left[f^{-1} \star g^{-1}\right]$

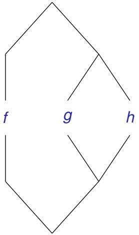
Thinking concretely

An operational view

1. Deal a deck of cards into two stacks, using ${\Omega_2}^{-1}$.
2. Apply f to Deck 0 and g to Deck 1.
3. Merge the results, using the riffle shuffle Ω_2.

We draw this in the natural way as $[f \star g] =$ 

and interpret bracketing as tree structure, so $[f \star [g \star h]]$ is given by 

$=$ 

Associators for Girard's conjunction

Note that $[\_ \star \_]$ is not associative. In general, $[f \star [g \star h]] \neq [[f \star g] \star h]$.

A general principle :

No injective homomorphism $M \times M \to M$ on a non-abelian monoid can satisfy this condition.

"Coherence and Strictification for Self-Similarity"
(PMH) *Journal of Homotopy & Related Structures* 2016

Instead, it is associative 'up to conjugation by a fixed element'

$$[[f \star g] \star h] = \alpha\, [f \star [g \star h]]\, \alpha^{-1}$$

- This 'fixed element' is the associator $\alpha = \gamma_L \gamma_R^{-1}$ derived from $\mathcal{K}_3$.
- It is one of the two generators of $\mathcal{F}$.
- The other generator of $\mathcal{F}$ is simply $[Id \star \alpha]$.

Mapping between **adjacent** vertices?

The connection between associativity isomorphisms and the 1-skeletons (i.e. vertices and edges) of associahedra is well-known :

> *"Given any n objects of a monoidal category, the associativity isomorphisms give a [commuting] diagram whose shape is the 1-skeleton of K_n"*
>
> — *M. Kapranov (1993)*

What about when the category in question only has one object??

All vertices are labeled by the same object — and paths between them are labeled by members of the same group (i.e. Thompson's $\mathcal{F}$) of associativity isomorphisms.

In our setting: Each associahedron K_n determines a commuting diagram of congruential bijections on $\mathbb{N}$.

How this is done ...

For each edge of K_n between n-leaf binary trees T_1 and T_2 :

- First choose a direction
$$\begin{tikzcd} & T_1 \arrow[dl] \\ T_2 & \end{tikzcd}$$
  (It is usual to base this on the Tamari ordering)

- Label the edge by the 'corresponding rearrangement'
$$\begin{tikzcd} & T_1 \arrow[dl, "\ulcorner T_2 \urcorner \ulcorner T_1 \urcorner^{-1}"] \\ T_2 & \end{tikzcd}$$

- Finally, replace every vertex by the natural numbers
$$\begin{tikzcd} & \mathbb{N} \arrow[dl, "\ulcorner T_2 \urcorner \ulcorner T_1 \urcorner^{-1}"] \\ \mathbb{N} & \end{tikzcd}$$

$\mathcal{K}_4$ — MacLane's pentagon

$$
\begin{tikzcd}
& \mathbb{N} \arrow[dl, "\alpha"'] & \\
\mathbb{N} & \text{COMMUTES} & \mathbb{N} \arrow[ul, "\alpha"'] \arrow[dl, "Id \star \alpha"] \\
\mathbb{N} \arrow[u, "\alpha \star Id"] & \mathbb{N} \arrow[l, "\alpha"] &
\end{tikzcd}
$$

$$
n \mapsto \begin{cases} 4n & n \ (mod\ 2) = 0 \\ n+2 & n \ (mod\ 4) = 1 \\ \frac{n+1}{2} & n \ (mod\ 8) = 3 \\ \frac{n-3}{4} & n \ (mod\ 8) = 2 \end{cases}
$$

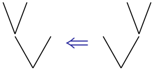
We may check arithmetically ...

This is MacLane's famous **pentagon condition** : $\alpha^2 = (\alpha \star Id)\alpha(Id \star \alpha)$

Question : In arbitrary associahedra, which elements of $\mathcal{F}$ end up labeling edges?

A non-minimal generating set

Recall : Two vertices are adjacent iff (equivalently)

1. We may remove a pair of brackets from each to get the same edge-label
   $(\bullet(\bullet\bullet)) \Longrightarrow (\bullet\bullet\bullet) \Longleftarrow ((\bullet\bullet)\bullet)$
2. We may map one to the other by a single rebracketing. 

The “symmetric generating set” of $\mathcal{F}$

Introduced by P. Dehornoy (2011), and may be characterised by

“Pairs of trees that differ by a single rotation *[application of associativity]*”

— this precisely captures mappings between *adjacent vertices*.

Characterising Dehornoy's generators, categorically

P. Dehornoy introduced his generating set in terms of "indexings of subtrees by finite binary sequences".

We may understand these categorically, via Girard's tensor :

An inductive definition

We characterise Dehornoy's generators $\mathcal{D}$ by

1. $\alpha \in \mathcal{D}$.
2. Given $d \in \mathcal{D}$, then $[1 \star d]$, $[d \star 1] \in \mathcal{D}$.

i.e. The closure of the associator under the functors $[Id \star \_]$ and $[\_ \star Id]$.

We may then interpret his binary strings as describing repeated applications of the injective homomorphisms $[Id \star \_]$, $[\_ \star Id]$: $\mathcal{I}_{\mathbb{N}} \rightarrow \mathcal{I}_{\mathbb{N}}$ to the associator α.

Thompson's $\mathcal{F}$ is the free, monogenic, monoid-with-tensor.

A fun application ...

Associahedra & operads in cryptography

Two questions :

1. Would it be wise to base a cryptosystem on a “free monogenic structure”?
2. What – if anything – is the connection between
   1. Thompson’s group $\mathcal{F}$
   2. Prime factorisations?

Some relevant references :

- **Combinatorial group theory and public key cryptography**
  V. Shpilrain & G. Zapata (2004)
  Commuting Action Key Exchange (CAKE) – a generic proposal for cryptosystems based on algebraic structures.
- **Thompson's group $\mathcal{F}$ and Public Key Cryptography**
  — *V. Shpilrain & A. Ushakov (2004)*
  "This group has several properties that make it particularly fit for cryptographic purposes"
- **The Shpilrain-Ushakov Protocol is always breakable**
  — *F. Matucci (2006)*
- **Length-Based Cryptanalysis: the case of Thompson's group**
  — *Ruinskiy, Shamir, Tsaban (2007)*
  "no practical public key cryptosystem based on the difficulty of solving an equation in this group can be secure."

Why study a dead protocol??

One interesting comment needs to be considered :

> *The difficulty of solving equations "resembles the factorization problem at the heart of the RSA cryptosystem."* — Shpilrain & Ushakov (2004)

The combination of always breakable and resembles RSA should perhaps be investigated further ...

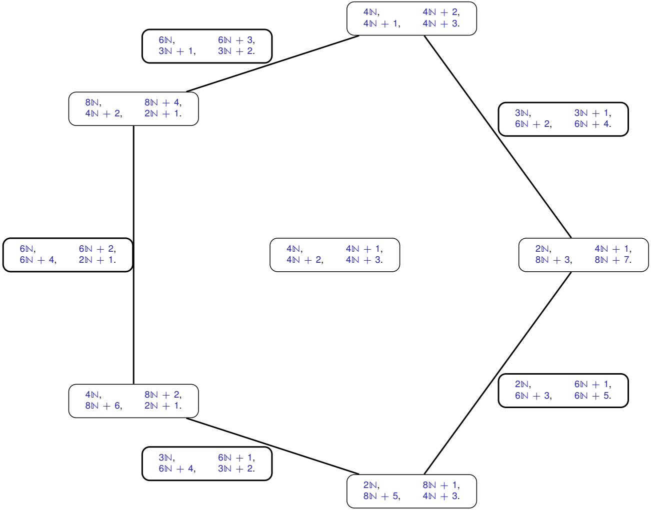
Some significant previous work

- "Arithmetree" (2001) — J.-L. Loday's *non-commutative arithmetic* based on associahedra and planar trees.
- "The arithmetic of trees" (2008) – A. Bruno, D. Yasaki consider *primes & factorisations* within Loday's system.

Is it possible that Thompson's $\mathcal{F}$, in a disguised manner, is manipulating prime factorisations?

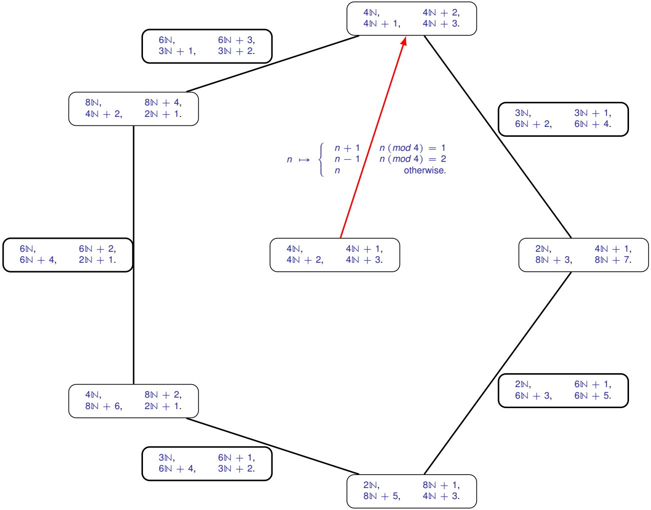
Labeling $\mathcal{K}_4$ with (ordered) finite open covers of $\mathbb{N}$

Our starting point is labeling $\mathcal{K}_4$ (the whole of it .. not just MacLane's pentagon) with ordered finite open covers of $\mathbb{N}$



This makes it easy to just write down the rearrangements.

Particularly simple rearrangements



One rearrangement stands out as *particularly simple*.

Additive rearrangements on $\mathbb{N}$

A rearrangement θ is K**-additive** for some $K > 0$ when there exists some set of integers $\{-K < x_i < K\}_{i=0..K-1} \subseteq \mathbb{Z}$ such that

$$\theta(n) = n + x_j \ \ \forall \ \ n \ (mod\ K) = j$$

Simple properties :

θ is K-additive $\Rightarrow$

1. $\theta(K+n) = K + \theta(n)$, for all $n \in \mathbb{N}$.
2. it is also KT-additive, for all $T > 0$.
3. it is uniquely determined by its action on $\{0, \ldots, K-1\}$.
4. the orbit of every natural number under θ is **bounded**. For all $n \in \mathbb{N}$,

$$\theta^L(n) = n \quad \text{for some} \quad L \leqslant K$$

Another monoid operation on operads

For all $A \in \mathcal{R}iff_m$ and $B \in \mathcal{R}iff_n$, we define $A \otimes B \in \mathcal{R}iff_{m \times n}$ to be the result of

"Grafting a copy of B onto every leaf of A."

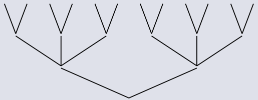
Formally : $A \otimes B \; = \; ((\ldots((A \circ_m B) \circ_{m-1} B) \circ_{m-2} \ldots) \circ_1 B)$.

Note that $\_ \otimes \_$ is strictly associative and has an identity; $(\mathcal{X}, \otimes)$ is a monoid.

Remark : We may think of this as a (strict) categorical tensor on the groupoid $\mathbb{RPT}$

Illustrative example :

The operation $\Omega_2 \otimes \Omega_3 \otimes \Omega_2 \; \in \; \mathcal{R}iff_{12}$ is given by



This is determined by the *ordered* factorisation $12 = 2 \times 3 \times 2$.

Rearrangements from prime factorisations

Consider distinct primes $P \neq Q \in \mathbb{N}$, together with the associahedron $\mathcal{K}_{PQ}$.

The shuffles $\Omega_P \otimes \Omega_Q \in \mathcal{R}iff_{PQ}$ and $\Omega_Q \otimes \Omega_P \in \mathcal{R}iff_{PQ}$ are then *distinct* facets of the associahedron $\mathcal{K}_{PQ}$, and there are (non-identity) paths between them.

Proposition The composite along any such path is an additive rearrangement.

(Outline) Proof : From the explicit description of members of $\mathcal{R}iff$,

$$(\Omega_P \otimes \Omega_Q)(n,i) \;=\; PQn + \sigma(i) \quad \text{and} \quad (\Omega_Q \otimes \Omega_P)(n,i) \;=\; QPn + \tau(i)$$

for some *distinct* permutations σ, τ on $\{0, \ldots, PQ-1\}$.

Composing gives,

$$(\Omega_P \otimes \Omega_Q)(\Omega_Q \otimes \Omega_P)^{-1}(n) \;=\; PQ\left(\frac{n-\tau(i)}{QP}\right) + \sigma(i) \;=\; n + (\sigma(i) - \tau(i))$$

for some $0 \leqslant i < PQ$

Can $\mathcal{F}$ be manipulating such factorisations?

Not all additive rearrangements in $\mathcal{K}_n$ come from (ordered) prime factorisations of n. Every associahedron $K_{n\geq 4}$ has paths labeled by additive rearrangements, simply because $\mathcal{R}_4 \hookrightarrow R_5 \hookrightarrow \mathcal{R}_6 \hookrightarrow \ldots$

Question : Can any of these live on the 1-skeleton – and thus form part of Thompson's $\mathcal{F}$, and so play a rôle in the Shpilrain-Ushakov protocol ?

The only additive rearrangement in $\mathcal{F}$ is the identity

Binary trees where the all leaf-edge paths have the same length are of the form $\Omega_2 \otimes \Omega_2 \otimes \ldots \otimes \Omega_2$ — we get at most one per associahedron.

An interesting (Collatz / Conway -style) distinction ?

- The orbit of every natural number, under a rearrangement determined by a prime factorisation, is **bounded**.
- ("Conjecture") The torsion-freeness of $\mathcal{F}$ implies that for every element $f \neq I \in \mathcal{F}$, there exists some $x \in \mathbb{N}$ whose orbit under f is **unbounded**.

Rearrangements as canonical coherence isomorphisms

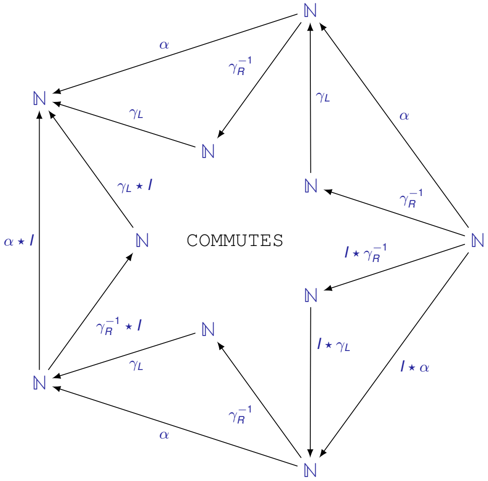
In ‘traditional’ settings the Collatz operators are *hidden*

— they occur in matching pairs that make up the associator.

When we move beyond the 1-skeleton, this is no longer the case!

A Commuting Pentagram

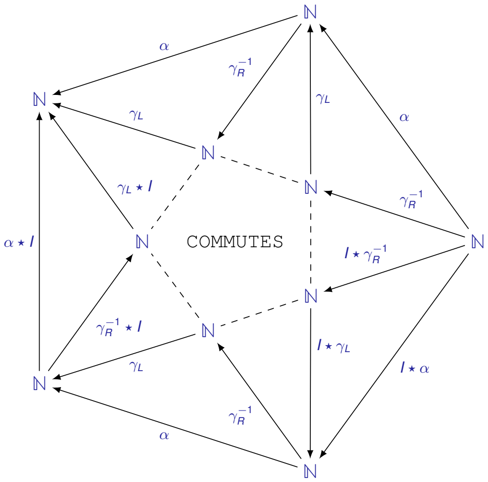
Let us take MacLane's pentagon over Thompson's $\mathcal{F}$, with Girard's conjunction, and add in the factorisation of the associator as Collatz bijections :



(i.e. including the rearrangements between *vertices* and *edges*).

A Commuting Pentagram

Looking at the inner pentagon, we recover the rearrangements between *edges* :



Another commuting Pentagon

A commuting diagram of rearrangements between *edges* :

$$
\begin{tikzcd}
 & \mathbb{N} \arrow[ddl, "(\gamma_L^{-1} \star I)\gamma_L"'] & \\
 & & \mathbb{N} \arrow[ul, "\gamma_R^{-1}\gamma_L = \alpha^{-1}"'] \\
\mathbb{N} & \texttt{COMMUTES} & \\
 & & \mathbb{N} \arrow[uu, "\gamma_R^{-1}(I \star \gamma_R)"'] \arrow[dl, "\gamma_R^{-1}(I \star \gamma_L)"] \\
 & \mathbb{N} \arrow[uul, "(\gamma_R \star I)\gamma_L"] &
\end{tikzcd}
$$

A suitable setting ??

We could continue, and consider :

- Mappings between edges in arbitrary $\mathcal{K}_n$,
- Mappings between higher-dimensional facets (faces, volumes, etc.) of $\mathcal{K}_n$

It is worthwhile to take a more structural approach, and ask :

For what setting is this describing a form of coherence?

The route to this is through generalising Girard's conjunction

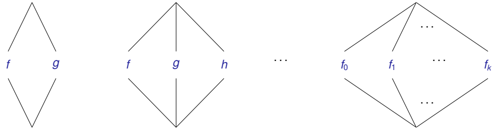
When viewed in terms of card shuffles, it is natural to consider Girard's conjunction to be the first of a series of homomorphic embeddings

$$\overbrace{[\_ \star \_ \ldots \_ \star \_]}^{k \text{ times}} : (\mathcal{I}_{\mathbb{N}})^{\times k} \hookrightarrow \mathcal{I}_{\mathbb{N}} \quad \text{for all } k \in \mathbb{N}$$

and indeed, view these as defining an operad.

Generalising conjunctions

We generalise Girard's conjunction to the following injective homomorphisms, given by conjugation by Ω_K.



The intuition :

A deck of cards is split into k decks using the deal Ω_k^{-1}. Maps $f_0, f_1, \ldots, f_{k-1}$ are applied to the respective decks, which are then shuffled together using Ω_K.

Writing this out explicitly,

$$[f_0 \star f_1 \star \ldots \star f_{k-1}](n) \;=\; k.f_r\left(\frac{n-r}{k}\right) + r \;\; where \;\; n \; (mod \; k) = r$$

Each of these defines an *injective inverse semigroup homomorphism*.

Generalised conjunctions as an operad

Define $\mathcal{BOB}$, the operad of **Bobzien Conjunctions**[4] $\mathcal{BOB}$ to be generated by

$$\{Id\ ,\ [\_ \star \_]\ ,\ [\_ \star \_ \star \_]\ ,\ [\_ \star \_ \star \_ \star \_]\ ,\ \ldots\}$$

It is a sub-operad of the endomorphism operad of $\mathcal{I}_{\mathbb{N}}$ in the monoidal category $(\mathbf{Inv}, \times)$ of inverse monoids with Cartesian product.

Note : it is *freely generated* by one generator of each arity.

[4] As an explanation for the terminology, please see “The Combinatorics of Stoic Conjunction”, S. Bobzien, Oxford Studies in Ancient Philosophy (2011)

The key properties

1. Bobzien Conjunctions preserve compositions & identities.

Yes – they are homomorphisms!

The key properties

1. Members of $\mathcal{BOB}$ preserve compositions & identities.
2. The set $\mathcal{R}$ of rearrangements is closed under members of $\mathcal{BOB}$.

Outline :

We only need to show this for generators of $\mathcal{BOB}$.

Consider some $TS^{-1} \in \mathcal{R}_N$ along with $\Omega_K \in \mathcal{R}iff_k$. Then by definition

$$[Id \star \ldots \star (TS^{-1}) \star \cdots \star Id] = (\Omega_K \circ_j T)(\Omega_K \circ_j S)^{-1}$$

for some $0 \leqslant j < k$; this is a member of $\mathcal{R}_{N+k-1}$.

We may then appeal to the fact that $[\_ \star \ldots \star \_]$ is a homomorphism.

The key properties

1. Members of $\mathcal{BOB}$ preserve compositions & identities.
2. The set of rearrangements is closed under members of $\mathcal{BOB}$.
3. Arbitrary re-bracketings arise via conjugation by members of $\mathcal{R}$.

This is *by construction*.

In $\mathcal{BOB}_2, \mathcal{BOB}_3$ we have :

rebracketing via the associator $\alpha[f \star [g \star h]]\alpha^{-1} = [[f \star g] \star h]$

removing brackets via the right Collatz operator

$$\gamma_R^{-1}[f \star [g \star h]]\gamma_R = [f \star g \star h]$$

adding brackets via (the inverse of) the left Collatz operator

$$\gamma_L[f \star g \star h]\gamma_L^{-1} = [[f \star g] \star h]$$

The key properties

1. Members of $\mathcal{BOB}$ preserve compositions & identities.
2. The set of rearrangements is closed under members of $\mathcal{BOB}$.
3. Arbitrary re-bracketings arise via conjugation by members of $\mathcal{R}$.
4. Rebracketings are unique.

Consider $\Gamma \neq \Delta \in \mathcal{BOB}_k$, and $\lambda, \mu \in \mathcal{R}_k$ that satisfy

$$\lambda^{-1}\Gamma(\_,\ldots,\_)\lambda \ = \ \Delta(\_,\ldots,\_) \ = \ \mu^{-1}\Gamma(\_,\ldots,\_)\mu$$

Then here exist some $P, Q \in \mathcal{R}\mathit{iff}_k$ such that

$$\Gamma(\_,\ldots,\_) = P(\_,\ldots,\_)P^{-1} \ \text{and}\ \Delta = Q(\_,\ldots,\_)Q^{-1}$$

As the operad $\mathcal{R}\mathit{iff}$ is freely generated, $\lambda = QP^{-1} = \mu$

The key properties

1. Members of $\mathcal{BOB}$ preserve compositions & identities.
2. The set $\mathcal{R}$ of rearrangements is closed under members of $\mathcal{BOB}$.
3. Arbitrary re-bracketings arise via conjugation by members of $\mathcal{R}$.
4. Rebracketings are unique.
5. All diagrams over $\mathcal{R}$ determined by paths through associahedra are guaranteed to commute.

   — this was our starting point.

A final question!

The operad $\mathcal{BOB}$ of Bobzien Conjunctions is isomorphic to

- The formal operad of *rooted planar trees*
- $\mathcal{R}iff$, the operad of *hierarchical riffle shuffles*.

Can we label the facets of the associahedron $\mathcal{K}_n$ by the generalised conjunctions in $\mathcal{BOB}_n$, consider mappings between these, and start the whole process again??

No : Bobzien Conjunctions are *injections*, but not *isomorphisms*.

A very bizarre fact

In a more general setting (i.e. Rings, rather than inverse semigroups) we may do exactly that.

"An Application of Polycyclic Monoids to Rings" — PMH , M. V. Lawson (1996)

gives necessary and sufficient conditions for a ring R to be isomorphic to all matrix rings $M_n(R)$, for $n > 0 \in \mathbb{N}$. These arise directly from the bijections found in $\mathcal{R}iff$.

A final question!

The operad $\mathcal{BOB}$ of Bobzien Conjunctions is isomorphic to

- The formal operad of *rooted planar trees*
- $\mathcal{R}iff$, the operad of *hierarchical riffle shuffles*.

Can we label the facets of the associahedron $\mathcal{K}_n$ by the generalised conjunctions in $\mathcal{BOB}_n$, consider mappings between these, and start the whole process again??

No : Bobzien Conjunctions are *injections*, but not *isomorphisms*.

A very bizarre fact

In a more general setting (i.e. Rings, rather than inverse semigroups) we may do exactly that.

"An Application of Polycyclic Monoids to Rings" — PMH , M. V. Lawson (1996)

gives necessary and sufficient conditions for a ring R to be isomorphic to all matrix rings $M_n(R)$, for $n > 0 \in \mathbb{N}$. These arise directly from the bijections found in $\mathcal{R}iff$.