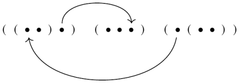
On Conway's proof of undecidability in elementary arithmetic

Peter M. Hines — Univ. York

Structure meets Power @ L.I.C.S.

Boston – June 2023



Au fond de l'Inconnu pour trouver du nouveau!

Talk based on a series of papers (2022-23)

- On Strict Extensional Reflexivity in Compact Closed Categories (in *Samson Abramsky on Logic & Structure in C.S. and beyond*)
  Outstanding Contributions to Logic (published, May 2023)
  `https://link.springer.com/book/9783031241161`
- On the Combinatorics of Interaction, *(submitted 2023)*
- The Inverse Semigroup Theory of Elementary Arithmetic *(submitted 2022)*
  `www.arxiv.org/abs/2206.07412`
- Congruential Functions as Categorical Coherence *(submitted 2022)*
- From a Conjecture of Collatz to Thompson's Group F,
  via a Conjunction of Girard `www.arxiv.org/abs/2202.04443`
- The Algebra and Category Theory of Elementary Arithmetic,
  (Looking for a home(!) 2023)
- A Simple Game – card shuffles, from conjectures of Collatz to modern mathematics & theoretical computer science *(Draft Book-in-Progress)*

An low-level programming language introduced by John H. Conway (1987)

Syntax Programs are (finite?) lists of positive rationals :

$$\left[\frac{P_0}{Q_0} , \frac{P_1}{Q_1} , \frac{P_2}{Q_2} , \frac{P_3}{Q_3} , \ldots \right]$$

Execution **Input** is a positive natural number $n \in \mathbb{N}^+$

The iterated step :

- Try to multiply n by each $\frac{P_0}{Q_0} , \frac{P_1}{Q_1} , \frac{P_2}{Q_2} , \frac{P_3}{Q_3} , \ldots$ in turn,

  until a whole number $n \times \frac{P_j}{Q_j} \in \mathbb{N}^+$ is found.
- replace n by this number $n \leftarrow n \times \frac{P_j}{Q_j}$

Conditional looping The above step is repeated,

until the end of the list is reached.

Output The final value of n, at the end of the list.

Registers and conditionals from prime factorisations

(The F.T.A.) Every $n \geqslant 1$ admits a **unique prime decomposition** :

$$n = 2^{x_2} \times 3^{x_3} \times 5^{x_5} \times 7^{x_7} \times 11^{x_{11}} \times \ldots$$

where a finite number of these exponents $\{x_j\}_{j \in \texttt{primes}}$ are non-zero.

Think of these as **registers**, indexed by **primes**.

Each fraction becomes a **conditional**, an **increment** and a **branch**

$$\frac{15125}{189} = \frac{5^3 \times 11^2}{3^3 \times 7^1}$$

$\texttt{COND}\ (x_3 \geqslant 3\ \texttt{AND}\ \ x_7 \geqslant 1)$

$\{x_5 \mapsto x_5 + 3;$
$x_{11} \mapsto x_{11} + 2;$
$\texttt{BRANCH}; \}$

FRACTRAN is resource-sensitive

Conditionals Consume Resources : A (successful) conditional $(x_j \geqslant M)$ decrements the **register** by the **test value** $x_j \mapsto x_j - M$.

There is a duality between *conditionals* and *assignments*;
this is enough to give computational universality.

A computationally universal FRACTRAN program

The 'Eval' program :

$$\frac{583}{559} \quad \frac{629}{551} \quad \frac{437}{527} \quad \frac{82}{517} \quad \frac{615}{329} \quad \frac{371}{129} \quad \frac{1}{115} \quad \frac{53}{86} \quad \frac{43}{53} \quad \frac{23}{47} \quad \frac{341}{46} \quad \frac{41}{43}$$

$$\frac{47}{41} \quad \frac{29}{37} \quad \frac{37}{31} \quad \frac{299}{29} \quad \frac{47}{23} \quad \frac{161}{15} \quad \frac{527}{19} \quad \frac{159}{7} \quad \frac{1}{17} \quad \frac{1}{13} \quad \frac{1}{3}$$

For every partial recursive function $f : \mathbb{N} \to \mathbb{N}$, there exists some natural number $Name_f \in \mathbb{N}$ such that

$$Name_f \times 2^{2^n} \xrightarrow{\texttt{Eval}} 2^{2^{f(n)}}$$

when $f(n)$ is defined, and fails to terminate otherwise.

Corollary It is *undecidable* whether Eval halts on a given input.

"What is the simplest Collatz-style game that we can expect to be undecidable? I think I have an answer!"

– Unsettleable Arithmetic Problems, (John Conway 2012)

Why “Collatz-style games” ??

Conway’s classic *Unpredictable Iterations* (1971) paper[1] exhibited

undecidability of iterative problems on **congruential functions**.

These are defined “piece-wise linearly on modulo classes”

Step 1. Dissect the natural numbers into the union of Modulo Classes

$$\mathbb{N} \;=\; A_0\mathbb{N}+B_0 \;\cup\; A_1\mathbb{N}+B_1 \;\cup\; A_2\mathbb{N}+B_2 \;\cup\; \ldots$$

(An ‘exact covering system’ in the sense of P. Erdös).

Step 2. Apply a distinct (rational) linear map to each modulo class,

$$f(n) \;=\; P_i n + Q_i \quad \text{where} \quad n \equiv B_i \mod A_i$$

such that $f(n) \in \mathbb{N}$.

[1] See also Sergei Maslov, *On E. L. Post’s Tag Problem* (1964)

What is this "simplest undecidable game"?

The **Notorious Collatz Conjecture** : $x \mapsto \begin{cases} \frac{x}{2} & x \text{ even,} \\ 3x+1 & x \text{ odd.} \end{cases}$

(Conjecture: every iterated sequence eventually arrives at 1).

The **Original Collatz Conjecture** (L. C., unpublished notebooks, 1 July, 1932).

J. Conway's '**Amusical Permutation**'

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

(Conjecture: This function has infinite orbits – the orbit of 8 is ∞).

The *Original* Collatz Conjecture was Conway's candidate for

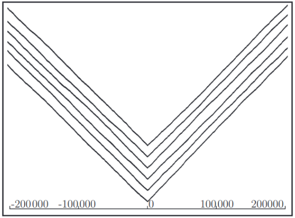
"The simplest undecidable (& therefore 'true') arithmetic statement."

Melodic Conjectures?

A “probvious” conjecture!

“The proportion of fallacies in published proofs is far greater than the small positive probability that [this conjecture is false]”
– *J.C.*, Unsettleable Algebraic Problems *(2012)*

A plot of $n \ : \ log\left(\gamma^n(k)\right)$, for $k = 8, 14, 40, 64, 80, 82$



$$\gamma^{200000}(8) \approx 10^{5000}$$

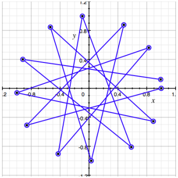
It goes like this, the fourth, the fifth ...

> *"There are twelve notes per octave, which represents a doubling of frequency, just as twelve steps [of γ or γ^{-1}] approximately doubles a number, on average."* — J.C. (2012)

This average-case doubling is not **exact** :

- [The amusical permutation] doubles by a factor of $\frac{3^{12}}{2^{18}} \approx 2$
- [Its inverse] doubles by a factor of $\frac{2^{20}}{3^{12}} \approx 2$

"A frequency ratio of $\frac{3^{12}}{2^{19}}$ is called the **Pythagorean comma** and is the difference between enharmonically equivalent notes (e.g. $A^\sharp$ and $B^\flat$). So there really is a connection with music."



Exact doubling / the octave is given by their geometric mean $\sqrt{\frac{3^{12}}{2^{18}} \cdot \frac{2^{20}}{3^{12}}} = 2$.

The amusing musical permutation

"Since the series always ascends by a fifth, modulo octaves, it does not sound very musical. It has always amused me to call it amusical."

Conjectures as code??

The O.C.C. is undecided – possibly undecidable[2].

Nevertheless, what does it look like, as a `FRACTRAN` program?

The problem :

Every `FRACTRAN` program implements a **purely multiplicative** congruential function

$$f(n) \;=\; \frac{X_i}{Y_i} n + 0 \qquad n \equiv B_i \mod A_i$$

. . . rather neatly ruling out his motivating example!

A question: Can we instead interpret these conjectures in other areas of theoretical computer science : logic / λ-calculus / category theory ???

[2] Although we could never prove undecidability(!)

Our claim : We should understand these conjectures in terms of **categorical logic** & **coherence**.

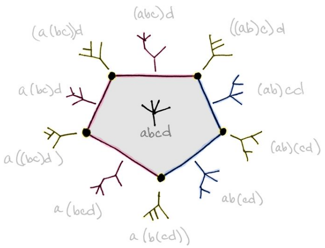
Today's Talk : The 'amusical permutation' is a

canonical coherence isomorphism

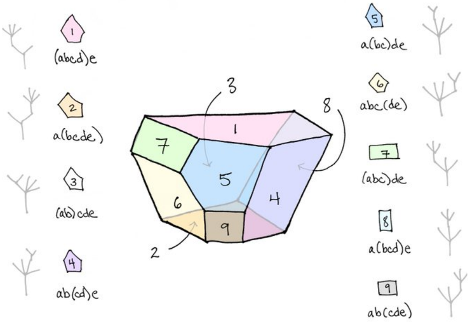
very closely related to associativity in models of linear logic.

The starting point for coherence for associativity

The Fourth Associahedron $\mathcal{K}_4$



The Fifth Associahedron $\mathcal{K}_5$



(Diagrams “borrowed” from Tai-Danae Bradley’s www.math3ma.com blog.)

We will label every facet (vertex, edge, face, . . .) of $\mathcal{K}_n$ by a distinct functor $\prod^n \mathcal{C} \to \mathcal{C}$.

Categories & functors

The (small) category in question

We work with the **symmetric group** $\mathcal{S}(\mathbb{N})$ of *bijections on natural numbers*[a].

[a] This is a subgroup of the **symmetric inverse monoid** $\mathcal{I}(\mathbb{N})$ of *partial injections* on the natural numbers, which is the correct setting, logically, algebraically, computationally, categorically, & group- and number- theoretically!

We equip $\mathcal{S}(\mathbb{N})$ with an $\mathbb{N}^+$-indexed family of *injective group homomorphisms*,

$$\star_k : \mathcal{S}(\mathbb{N})^{\times k} \hookrightarrow \mathcal{S}(\mathbb{N}) \qquad \forall\ k = 1, 2, 3, \ldots$$

These "**unbiased conjunctions**" are defined by :

$$\star_k(f_0, f_1, \ldots, f_{k-1})(kn + i) \ = \ k.f_i(n) + i \ \text{ where } i = 0, 1, 2, \ldots, k-1$$

Notation: We write $\star_k(f_0, \ldots, f_{k-1})$ as $(f_0 \star f_1, \star . \ldots \star f_{k-1})$.

A graphical formalism & explicit formulæ

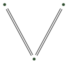
The Identity

$\star_1 : \mathcal{S}(\mathbb{N}) \to \mathcal{S}(\mathbb{N})$

$(f)(n) = f(n)$

Girard's conjunction

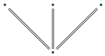
$\star_2 : \mathcal{S}(\mathbb{N}) \times \mathcal{S}(\mathbb{N}) \to \mathcal{S}(\mathbb{N})$



$$(f \star g)(n) = \begin{cases} 2.f\left(\frac{n}{2}\right) & n \text{ even,} \\ 2.g\left(\frac{n-1}{2}\right)+1 & n \text{ odd.} \end{cases}$$

Ternary conjunction

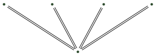
$\star_3 : \mathcal{S}(\mathbb{N})^{\times 3} \to \mathcal{S}(\mathbb{N})$



$$(f \star g \star h)(n) = \begin{cases} 3.f\left(\frac{n}{3}\right) & n \equiv 0 \mod 3 \\ 3.g\left(\frac{n-1}{3}\right)+1 & n \equiv 1 \mod 3 \\ 3.h\left(\frac{n-2}{3}\right)+2 & n \equiv 2 \mod 3 \end{cases}$$

4-ary conjunction

$\star_4 : \mathcal{S}(\mathbb{N})^{\times 4} \to \mathcal{S}(\mathbb{N})$



$$(f \star g \star h \star k)(n) = \begin{cases} 4.f\left(\frac{n}{4}\right) & n \equiv 0 \mod 4 \\ 4.g\left(\frac{n-1}{4}\right)+1 & n \equiv 1 \mod 4 \\ 4.h\left(\frac{n-2}{4}\right)+2 & n \equiv 2 \mod 4 \\ 4.k\left(\frac{n-3}{4}\right)+3 & n \equiv 3 \mod 4 \end{cases}$$

Why 'conjunctions'??

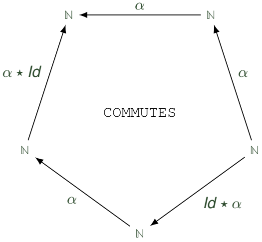
The binary case $(\_ \star \_) : \mathcal{S}(\mathbb{N}) \times \mathcal{S}(\mathbb{N}) \hookrightarrow \mathcal{S}(\mathbb{N})$ is a *categorical tensor* that models conjunction of MELL in J.-Y. Girard's 'Geometry of Interaction' (parts I, II).

It is associative up to **canonical isomorphism** $\alpha(n) = \begin{cases} 2n & n \equiv 0 \mod 2, \\ n+1 & n \equiv 1 \mod 4, \\ \frac{n-1}{2} & n \equiv 3 \mod 4, \end{cases}$

that satisfies

- **(Naturality)** $\alpha(f \star (g \star h)) = ((f \star g) \star h)\alpha$
- **(MacLane's Pentagon)** in the symmetric group $\mathcal{S}(\mathbb{N})$

$$\alpha^2 = (\alpha \star Id)\alpha(Id \star \alpha)$$



Why 'conjunctions'??

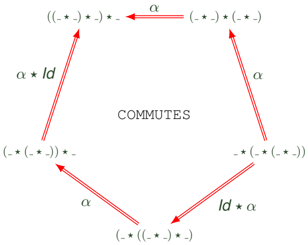
The binary case $(\_ \star \_) : \mathcal{S}(\mathbb{N}) \times \mathcal{S}(\mathbb{N}) \hookrightarrow \mathcal{S}(\mathbb{N})$ is a *categorical tensor* that models conjunction of MELL in J.-Y. Girard's 'Geometry of Interaction' (parts I, II).

It is associative up to **canonical isomorphism** $\alpha(n) = \begin{cases} 2n & n \equiv 0 \mod 2, \\ n+1 & n \equiv 1 \mod 4, \\ \frac{n-1}{2} & n \equiv 3 \mod 4, \end{cases}$

that satisfies

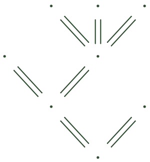
- **(Naturality)** $\alpha(f \star (g \star h)) = ((f \star g) \star h)\alpha$
- **(MacLane's Pentagon)** in the functor category $\mathbf{Grp}(\mathcal{S}(\mathbb{N})^{\times 4}, \mathcal{S}(\mathbb{N}))$

Natural iso.s between group hom.s



The general setting

By ‘plugging together’ unbiased conjunctions (substitution / operadic composition), we interpret k-leaf rooted planar trees as “**generalised conjunctions**” $\mathcal{S}(\mathbb{N})^{\times k} \hookrightarrow \mathcal{S}(\mathbb{N})$.

The tree	The homomorphism
	$((\_ \star (\_ \star \_ \star \_)) \star \_) \ : \ \mathcal{S}(\mathbb{N})^{\times 5} \hookrightarrow \mathcal{S}(\mathbb{N})$

Claim : Distinct trees determine distinct homomorphisms!

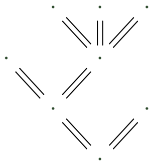
Formally : the unbiased conjunctions *freely generate* a non-symmetric sub-operad of the endomorphism operad of $\mathcal{S}(\mathbb{N}) \in Ob(\mathbf{Grp}, \times)$, isomorphic to the operad $\mathbb{RPT}$ of rooted planar trees.

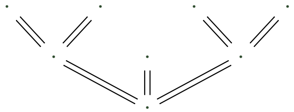
We can uniquely label arbitrary facets of associahedra by group homomorphisms :)

Mapping between generalised conjunctions

In order to turn **associahedra** into **commuting diagrams** we need (unique) natural isomorphisms between facets.

Consider gen. conjunctions $T, U : \mathcal{S}(\mathbb{N})^{\times 5} \hookrightarrow \mathcal{S}(\mathbb{N})$ (edges of $\mathcal{K}_5$)

$T =$ 

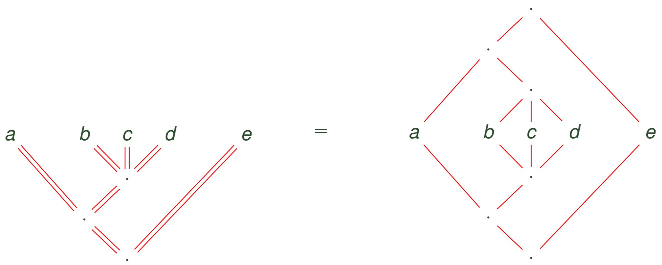
$U =$ 

We need some $\eta_{T,U} \in \mathcal{S}(\mathbb{N})$ such that

$$\eta_{T,U}.((\_ \star (\_ \star \_ \star \_)) \star \_) \quad = \quad ((\_ \star \_) \star \_ \star (\_ \star \_)).\eta_{T,U}$$

We find this by '**unfolding**' generalised conjunctions into *shuffles* and *deals* of an infinite pack of cards.

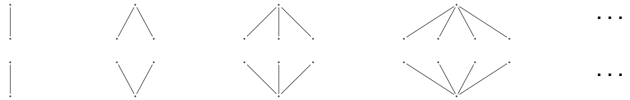
Unfolding the conjunction $(\ \star\_)\star\_\star(\_\star\_)) : \mathcal{S}(\mathbb{N})^{\times 5} \hookrightarrow \mathcal{S}(\mathbb{N})$.



into (operadic) composites of **shuffles** and **deals**

Fair Deals

Riffle shuffles



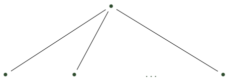
Games in Hilbert's Casino

Multiple decks of (countably infinitely many) cards are modelled by **disjoint union**

$$\biguplus^{k} \mathbb{N} \;=\; \mathbb{N}\times\{0\} \;\cup\; \mathbb{N}\times\{1\} \;\cup \ldots \cup\; \mathbb{N}\times\{k-1\}$$

(also a categorical tensor).

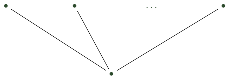
The k-player fair deal



$$n \mapsto \left(\frac{n-i}{k}, i\right)$$

where $n \equiv i \mod k$

The k-deck riffle shuffle

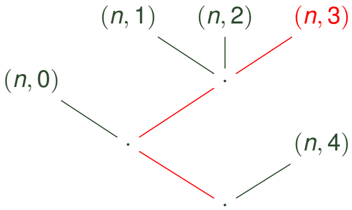


$$(n, i) \mapsto kn + i$$

These live within the endomorphism operad of the natural numbers, in the groupoid of bijections on sets, with (strict) disjoint union.

Linear maps from trees

Deriving the map $(n, 3) \mapsto 12n + 10$, from the leaf-to-root path :



Branch number 2 of 3

Branch number 1 of 2

Branch number 0 of 2

Multiplicative coefficient : $12 = 3 \times 2 \times 2$

Additive coefficient :	(Decimal)		Base 3	Base 2	Base 2
	10	$=$	2	1	0

Positional mixed-radix number systems

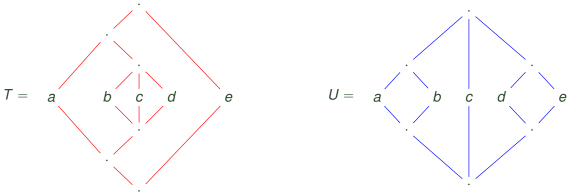
First formal study by G. Cantor, *Über einfache Zahlensysteme* (1869)

Constructing natural isomorphisms

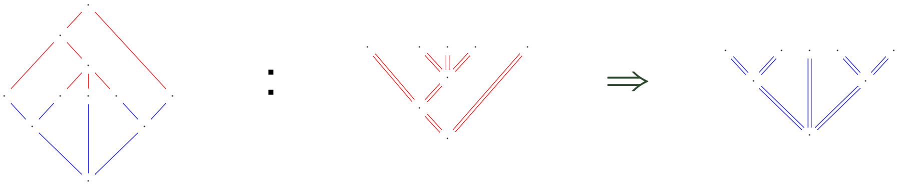
To find the natural isomorphism $\eta_{T,U} \in \mathcal{S}(\mathbb{N})$ from

$$T = ((\_ \star (\_ \star \_ \star \_)) \star \_) \quad \text{to} \quad U = ((\_ \star \_) \star \_ \star (\_ \star \_))$$

we simply unfold them both



then compose the **deal** from T with the **shuffle** from U, giving an element of $\mathcal{S}(\mathbb{N})$.



Concrete formulæ for congruential natural isomorphisms

Given explicit descriptions of generalised conjunctions :

- $T(f_0, f_1, \ldots f_{k-1})(A_i n + B_i) \ = \ A_i f_i(n) + B_i$,
- $U(f_0, f_1, \ldots f_{k-1})(C_i n + D_i) \ = \ C_i f_i(n) + D_i$,

where $i = 0, 1, \ldots, k-1$,

the natural isomorphism $\eta_{T,U} : T \Rightarrow U$ has the unique component

$$\eta_{T,U}(n) \ = \ \frac{1}{A_j}\left(C_j n + \begin{vmatrix} A_j & B_j \\ C_j & D_j \end{vmatrix} \right) \ \text{where} \ \ n \equiv B_j \mod A_j$$

This is a congruential element of $\mathcal{S}(\mathbb{N})$.

A posetal groupoid, with unbiased tensors

Simple properties :

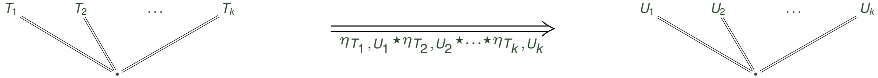
- $\eta_{T,T} = Id$.
- $\eta_{T,U}^{-1} = \eta_{U,T}$
- $\eta_{U,V}\eta_{T,U} = \eta_{T,V}$

We derive a **posetal groupoid** $\mathcal{A}$ (over which *'all diagrams commute'*).

Objects Generalised conjunctions $\mathcal{S}(\mathbb{N})^{\times k} \hookrightarrow \mathcal{S}(\mathbb{N})$
(in 1:1 correspondence with Rooted Planar Trees)

Arrows A unique natural iso. between any two conjunctions of the same arity
(i.e. any two facets of the same associahedron)

Unbiased tensors We have one of each arity ... $\prod^k \mathcal{A} \to \mathcal{A}$.

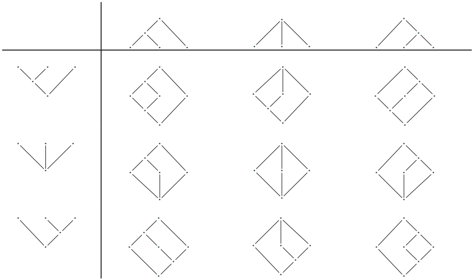


We may translate associahedra into commuting diagrams of congruential functions

A worked example : $\mathcal{K}_3$

The (unjustly neglected) third associahedron :

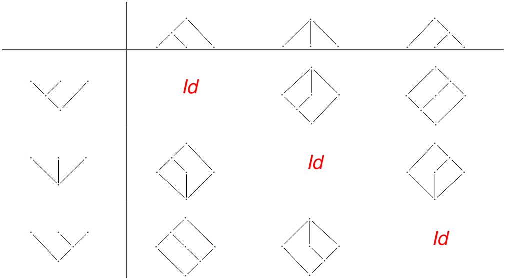
$$((\_ \star \_) \star \_) \xrightarrow{\;(\_\star\_\star\_)\;} (\_ \star (\_ \star \_))$$



A worked example : $\mathcal{K}_3$

The (unjustly neglected) third associahedron :

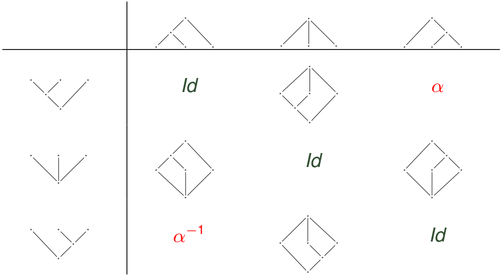
$$((\_ \star \_) \star \_) \xrightarrow{(\_\star\_\star\_)} (\_ \star (\_ \star \_))$$



Identities!

The (unjustly neglected) third associahedron :

$$((\_ \star \_) \star \_) \xrightarrow{(\_\star\_\star\_)} (\_ \star (\_ \star \_))$$



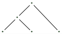
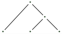
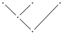
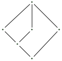
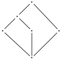
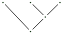
The associator for Girard's conjunction

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

A worked example : $\mathcal{K}_3$

The (unjustly neglected) third associahedron :

$$((\_ \star \_) \star \_) \xrightarrow{(\_\star\_\star\_)} (\_ \star (\_ \star \_))$$

			
	*Id*		α
		*Id*	γ^{-1}
	α^{-1}	γ	*Id*

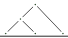
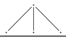
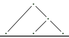
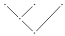
Conway's
amusical permutation
(from the O.C.C.)

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

A worked example : $\mathcal{K}_3$

The (unjustly neglected) third associahedron :

$$((\_ \star \_) \star \_) \xrightarrow{(\_\star\_\star\_)} (\_ \star (\_ \star \_))$$

			
	Id	$\gamma_\flat$	α
	$\gamma_\flat^{-1}$	Id	γ^{-1}
	α^{-1}	γ	Id

The **flattened permutation**

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

Satisfying

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

As a nat. transformation,

$$Succ.\gamma_\flat^M = \gamma^M.Succ$$

Simple Corollaries (I)

These can all be verified by elementary modular arithmetic

Every associahedron $\mathcal{K}_{N\geqslant 3}$ contains paths labelled by :

1. The associator α

   ("Right-to-Left rebracketing")

2. The amusical permutation γ

   ("Inserting brackets on the RHS")

3. The flattened permutation $\gamma_\flat$

   ("Inserting brackets on the LHS")

Simple Corollaries (II)

These can all be verified by elementary modular arithmetic

The associativity isomorphism for the multiplicative conjunction of Linear Logic
(from the Geometry of Interaction program)
may be written in terms of Conway's / Collatz's amusical permutation

"Right-to-Left rebracketing" = "Delete brackets on RHS"
then
"Insert brackets on LHS"

This gives $\alpha = \gamma_\flat \gamma^{-1}$.

$$\alpha(n) = \gamma(\gamma^{-1}(n) + 1) - 1$$

A Corollary of a Corollary

These can all be verified by elementary modular arithmetic

Richard Thompson's group $\mathcal{F}$, known[3] to be generated by the bijections

$$\{\alpha\ ,\ Id \star \alpha\} \subseteq \mathcal{S}(\mathbb{N})$$

can be described in terms of the Original Collatz Conjecture.

It is generated by

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

[3] from PMH 2023, based on Fiore & Leinster 2010, M.V. Lawson 2004, P. Dehornoy 1996, & long-established folklore ...

Vertices & edges of $\mathcal{K}_4$