

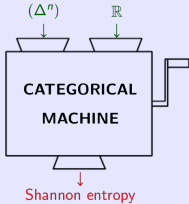
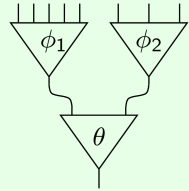
An algebraic view of entropy

Tom Leinster

University of Edinburgh

Three talks

Sunday: Operads



Monday: An algebraic view of entropy

Thursday: Entropy modulo a prime



Trajectory of these three talks

SUNDAY

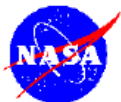
MONDAY

I will explain how operads—a cousin of algebraic theories—lead to the notion of entropy (which might seem to belong to other branches of science).

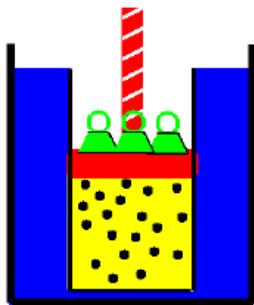
Then I will show how this story leads to a mysterious construction in number theory.

THURSDAY

Entropy in the sciences



Entropy of a Gas



S = Entropy

Q = Heat Transfer

T = Temperature

$$\text{2nd Law: } S_2 - S_1 = \frac{\Delta Q}{T}$$

$$\text{Differential 2nd Law: } dS = \frac{dQ}{T}$$

H = Enthalpy V = Volume p = Pressure

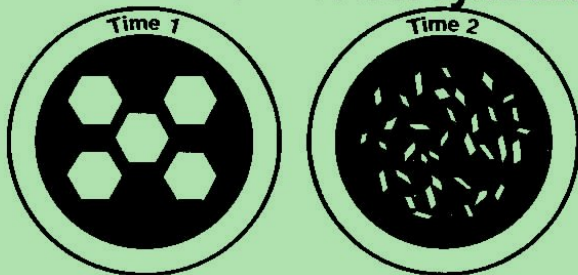
$$\text{Differential 1st Law: } dQ = dH - p dV$$

C_p = Heat Capacity
(constant pressure)

R = Gas Constant

Entropy in the sciences

Second Law of Thermodynamics



ENTROPY (simplicity) increases
in closed system



C_p = Heat Capacity
(constant pressure)

R = Gas Constant

Heat Transfer

$$Q = \frac{\Delta Q}{T}$$

$$= \frac{dQ}{T}$$

Pressure $p =$

$$= dH - V$$

Entropy in the sciences

Entropy Approach to the Investigation of Information Capabilities of Adaptive Radio Engineering System in Conditions of Intrasystem Uncertainty

V. V. Skachkov,* V. V. Chepkyi,** H. D. Bratchenko,*** and A. N. Efymchykov

Odessa State Academy of Technical Regulation and Quality, Odessa, Ukraine



Heat Tra

$$= \frac{\Delta Q}{T}$$

Minimum entropy control of nonlinear ARMA systems over a communication network

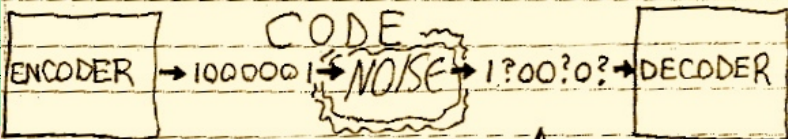
Jianhua Zhang · Hong Wang

c_p - heat capacity
(constant pressure)

n - gas con

Entropy in the sciences

NOISE AND INFORMATION ENTROPY



- LOW ENTROPY
- HIGH DEGREE OF CERTAINTY
- LOW DEGREE OF UNCERTAINTY

- HIGH ENTROPY
- LOW DEGREE OF CERTAINTY
- HIGH DEGREE OF UNCERTAINTY

Entropy in the sciences

NOISE AND INFORMATION ENTROPY

Entropy, the Central Limit Theorem and the Algebra of the Canonical Commutation Relation

DÉNES PETZ

Mathematical Institute HAS, H-1364 Budapest, PF 127, Hungary

- LOW ENTROPY
- HIGH DEGREE
OF CERTAINTY
- LOW DEGREE
OF UNCERTAINTY

- HIGH ENTROPY
- LOW DEGREE
OF CERTAINTY
- HIGH DEGREE
OF UNCERTAINTY

Entropy in the sciences

Entropy, the
Algebra of

DÉNES PETZ
Mathematical Institute

BAYESIAN INFERENCE AND MAXIMUM ENTROPY METHODS IN SCIENCE AND ENGINEERING

Proceedings of the 30th International Workshop
on Bayesian Inference and Maximum Entropy
Methods in Science and Engineering

4 - 9 July 2010 Chamonix, France

- HIGH DEGREE
OF CERTAINTY
- LOW DEGREE
OF UNCERTAINTY

- LOW DEGREE
OF CERTAINTY
- HIGH DEGREE
OF UNCERTAINTY

Entropy in the sciences

PROBABILISTIC KNOWLEDGE REPRESENTATION AND REASONING AT MAXIMUM ENTROPY BY SPIRIT

Carl-Heinz Meyer, Wilhelm Rödder
FernUniversität Hagen

Proceedings of the 30th International Workshop
on Bayesian Inference and Maximum Entropy
Methods in Science and Engineering

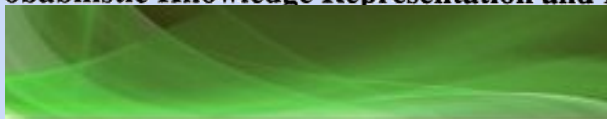
4 - 9 July 2010 Chamonix, France

- HIGH DEGREE
OF CERTAINTY
- LOW DEGREE
OF UNCERTAINTY

- LOW DEGREE
OF CERTAINTY
- HIGH DEGREE
OF UNCERTAINTY

Entropy in the sciences

PROBABILISTIC KNOWLEDGE REPRESENTATION AND REASONING



Muhammad Ali

Abdul Haseeb

Muhammad Bilal Bhatti

Artificial Intelligence

Design and Implementation of Entropy Based Artificially Immune Malware Detection System

OF UNCERTAINTY

OF UNCERTAINTY

Entropy in the sciences

Maximum Entropy and Ecology

A Theory of Abundance, Distribution, and Energetics

John Harte



Entropy in the sciences

Maximum Entropy and Ecology

*A Theory of Abundance, Distribution,
and Energetics*

**Impact of a Change of Support
on the Assessment of Biodiversity
with Shannon Entropy**

Didier Josselin¹, Ilene Mahfoud¹, Bruno Fady²



Entropy in the sciences

Roman F. Nalewajski

Reduced communication channels of molecular fragments and their entropy/information bond indices

An entropic characterization of protein interaction networks and cellular robustness

Thomas Manke, Lloyd Demetrius, Martin Vingron

M

Resilience and entropy as indices of robustness of water distribution networks

R. Greco, A. Di Nardo and G. Santonastaso

7 Algorithmic entropy and Kolmogorov complexity

Entropy and Quantum Kolmogorov Complexity: A Quantum Brudno's Theorem

Fabio Benatti¹, Tyll Krüger^{2,3}, Markus Müller², Rainer Siegmund-Schultze², Arleta Szkoła²

7 Algorithmic entropy and

Rényi Relative Entropies and Noncommutative L_p -Spaces

Anna Jenčová

Entropy and Quantum Kolmogorov Complexity. A Quantum Brudno's Theorem

Fabio Benatti¹, Tyll Krüger^{2,3}, Markus Müller², Rainer Siegmund-Schultze²,
Arleta Szkoła²

Entropy in the sciences

Entropy and
generators in ergodic
theory (Mathematics
lecture note series)

ov and

opies and
Spaces

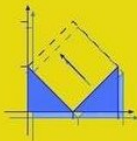
plexity.

iegmund-Schultze²,

Entropy in the sciences

Graham Everest and Thomas Ward

HEIGHTS OF POLYNOMIALS
AND ENTROPY IN
ALGEBRAIC DYNAMICS



new mathematical monographs: 18

Entropy in Dynamical
Systems

Tomasz Downarowicz

CAMBRIDGE

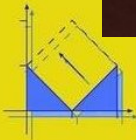
Entropy in the sciences

Graham Everest and

HEIGHTS OF POL

AND ENTRO

ALGEBRAIC DY



COMBINATORIAL DYNAMICS AND ENTROPY IN DIMENSION ONE

Second Edition

Investigation of chaotic
advection in the atmosphere:
the use of topological entropy

Tímea Haszpra

CAMBRIDGE

new mathematical monographs: 18

Entropy in Dynamical
Systems

Downarowicz

But in algebra and topology...



... you can go your whole life without ever using the word 'entropy'.

The point of this talk

Entropy is notable by its relative absence from algebra and topology.

However, we will see that by considering general algebraic structures such as operads and categories—and with just a *tiny* bit of topological input—we naturally arrive at entropy.

It's there, whether we like it or not!

The point of this talk

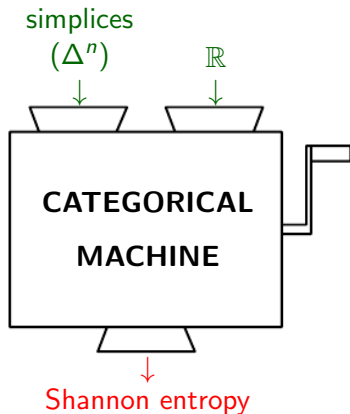


Image: J. Kock

The point of this talk

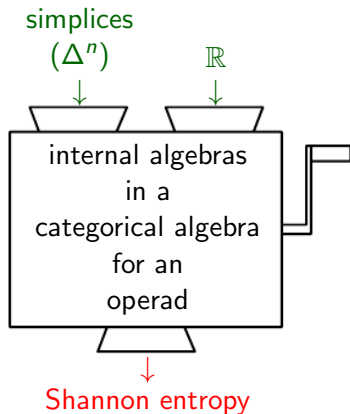


Image: J. Kock

Plan

1. What is entropy?
2. Review of yesterday
3. Categorical algebras for an operad
4. Internal algebras
5. The theorem: how entropy arises

I'll use a small amount of categorical vocabulary: category, functor, and (just once) natural transformation.

I'll also build on some of what I explained yesterday.

But even if you missed yesterday, come along for the ride...

1. What is entropy?

The definition of entropy

The simplest kind of entropy is the Shannon entropy of a finite probability distribution.

Let $\mathbf{p} = (p_1, \dots, p_n)$ be a finite probability distribution: so $p_i \geq 0$ and $\sum p_i = 1$.

Its (Shannon) entropy is

$$H(\mathbf{p}) = - \sum_{i=1}^n p_i \log p_i.$$

- When $p_i = 0$, interpret $0 \log 0$ as 0.
- Changing the base of the log only affects $H(\mathbf{p})$ up to a constant factor.

Entropy is the most important quantity associated with a probability distribution.

But what does it *mean*?

Entropy has a reputation for being mysterious. . .

My greatest concern was what to call it. I thought of calling it “information”, but the word was overly used, so I decided to call it “uncertainty”. When I discussed it with John von Neumann, he had a better idea. Von Neumann told me, “You should call it entropy, for two reasons. In the first place your uncertainty function has been used in statistical mechanics under that name, so it already has a name. In the second place, and more important, no one knows what entropy really is, so in a debate you will always have the advantage.”

—*Claude Shannon*

A lot of mystique surrounds entropy.

But it's not so mysterious!

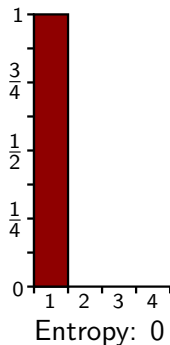
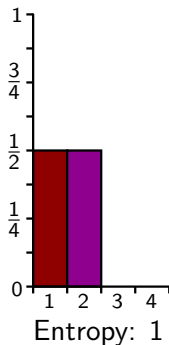
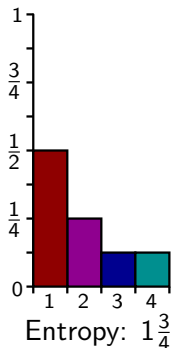
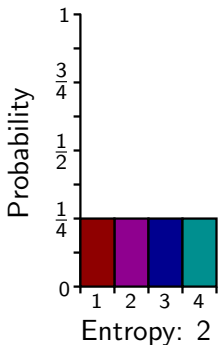
Entropy as uniformity

The entropy $H(\mathbf{p}) = -\sum p_i \log p_i$ can be understood as a measure of the *uniformity* of \mathbf{p} .

For distributions on an n -element set, its *maximum value* is $\log n$, achieved when $\mathbf{p} = (1/n, \dots, 1/n)$.

Its *minimum value* is 0, achieved when $\mathbf{p} = (0, \dots, 0, 1, 0, \dots, 0)$.

Examples with $n = 4$, taking logarithms to base 2:



2. Review of yesterday

The definition of operad

An **operad** is like an abstract clone, but without the reindexing of variables: it's a sequence $(P_n)_{n \geq 0}$ of sets together with:

- a **composition** operator

$$\begin{aligned} P_n \times P_{k_1} \times \cdots \times P_{k_n} &\rightarrow P_{k_1 + \cdots + k_n} \\ (\theta, \phi_1, \dots, \phi_n) &\mapsto \theta \circ (\phi_1, \dots, \phi_n) \end{aligned}$$

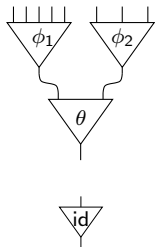
for each $n, k_1, \dots, k_n \geq 0$

- an **identity** element $\text{id} \in P_1$,

satisfying associativity and identity axioms.

Examples:

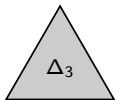
- **Terminal operad**: $P_n = \{*_n\}$ for all n .
- For any monoid M , get operad P^M with $P_1^M = M$ and $P_n^M = \emptyset$ otherwise.



The operad of simplices

The operad Δ of simplices:

$$\Delta_n = \{(p_1, \dots, p_n) \in \mathbb{R}^n : p_i \geq 0, \sum p_i = 1\}.$$



Composition is defined by thinking of $\mathbf{p} = (p_1, \dots, p_n)$ as a probability distribution on $\{1, \dots, n\}$. E.g. if

$$\mathbf{p} = \left(\text{coin} \right) = \left(\frac{1}{2}, \frac{1}{2} \right), \quad \mathbf{q}_1 = \left(\text{die} \right) = \left(\frac{1}{6}, \dots, \frac{1}{6} \right), \quad \mathbf{q}_2 = \left(\text{cards} \right) = \left(\frac{1}{52}, \dots, \frac{1}{52} \right)$$

then

$$\mathbf{p} \circ (\mathbf{q}_1, \mathbf{q}_2) = \left(\underbrace{\frac{1}{12}, \dots, \frac{1}{12}}_6, \underbrace{\frac{1}{104}, \dots, \frac{1}{104}}_{52} \right) \in \Delta_{58}.$$

Generally, given

$$\mathbf{p} = (p_1, \dots, p_n), \\ \mathbf{q}_1 = (q_1^1, \dots, q_1^{k_1}), \dots, \mathbf{q}_n = (q_n^1, \dots, q_n^{k_n}),$$

define

$$\mathbf{p} \circ (\mathbf{q}_1, \dots, \mathbf{q}_n) = (p_1 q_1^1, \dots, p_1 q_1^{k_1}, \dots, p_n q_n^1, \dots, p_n q_n^{k_n}) \in \Delta_{k_1 + \dots + k_n}.$$

Algebras for an operad

Let P be an operad.

A P -algebra is a set A together with a map

$$\bar{\theta}: A^n \rightarrow A$$

for each $n \geq 0$ and $\theta \in P_n$, satisfying action-like axioms:

- (i) composition, (ii) identity.

Examples:

- When P is the terminal operad, a P -algebra is exactly a monoid.
- An P^M -algebra is exactly a set with an M -action.
- Let $A \subseteq \mathbb{R}^d$ be a convex set. Then A becomes a Δ -algebra as follows: given $\mathbf{p} \in \Delta_n$, define

$$\begin{aligned} \bar{\mathbf{p}}: \quad A^n &\rightarrow A \\ (\mathbf{a}_1, \dots, \mathbf{a}_n) &\mapsto \sum_i p_i \mathbf{a}_i. \end{aligned}$$

Algebras in categories other than **Set**

Let \mathcal{M} be a category with some kind of product \otimes and unit object I : it could be (**Set**, \times , $\{*\}$), or something else.

Let P be an operad.

A P -algebra in \mathcal{M} is an object A of \mathcal{M} together with a map

$$\bar{\theta}: A^{\otimes n} \rightarrow A$$

for each $n \geq 0$ and $\theta \in P_n$, satisfying action-like axioms:

- (i) composition,
- (ii) identity.

Today, we'll think about the case where \mathcal{M} is **Cat**, the category of categories and functors.

3. Categorical algebras for operads

The definition of categorical algebra for an operad

Let P be an operad.

A **categorical P -algebra** is a P -algebra in **Cat**.

Explicitly: it's a category \mathbf{A} together with a functor

$$\bar{\theta}: \mathbf{A}^n \rightarrow \mathbf{A}$$

for each $n \geq 0$ and $\theta \in P_n$, satisfying action-like axioms:

- (i) composition, (ii) identity.

For $\bar{\theta}$ to be a **functor** $\mathbf{A}^n \rightarrow \mathbf{A}$ means:

- for all objects a_1, \dots, a_n of \mathbf{A} , we get an object $\bar{\theta}(a_1, \dots, a_n)$ of \mathbf{A}
- for all maps $f_1 \downarrow_{b_1}^{a_1}, \dots, f_n \downarrow_{b_n}^{a_n}$ in \mathbf{A} , we get a map $\bar{\theta}(f_1, \dots, f_n) \downarrow_{\bar{\theta}(b_1, \dots, b_n)}^{\bar{\theta}(a_1, \dots, a_n)}$ in \mathbf{A} ,

and that some axioms are satisfied.

Examples of categorical algebras

- Let P be the terminal operad: $P_n = \{*_n\}$ for all $n \geq 0$.

By definition, a categorical P -algebra is a category \mathbf{A} with a functor $\mathbf{A}^n \rightarrow \mathbf{A}$ for each $n \geq 0$, satisfying axioms.

It's exactly a strict monoidal category: a category equipped with a strictly associative and unital product \otimes . The functor $\overline{*_n}: \mathbf{A}^n \rightarrow \mathbf{A}$ is

$$(a_1, \dots, a_n) \mapsto a_1 \otimes \cdots \otimes a_n.$$

- Let M be a monoid and $P = P^M$ (so $P_1^M = M$ and $P_n^M = \emptyset$ otherwise).

A categorical P^M -algebra is a category \mathbf{A} with a functor $m \cdot - : \mathbf{A} \rightarrow \mathbf{A}$ for each $m \in M$, satisfying axioms.

It's exactly a category with an M -action.

More examples of categorical algebras

Take the operad Δ of simplices:

$$\Delta_n = \{(p_1, \dots, p_n) \in \mathbb{R}^n : p_i \geq 0, \sum p_i = 1\}.$$

We've already seen that the **set** \mathbb{R} is a Δ -algebra: for $\mathbf{p} \in \Delta_n$, define

$$\begin{aligned} \bar{\mathbf{p}}: \quad \mathbb{R}^n &\rightarrow \mathbb{R} \\ (a_1, \dots, a_n) &\mapsto p_1 a_1 + \dots + p_n a_n. \end{aligned}$$

Crucial point A one-object category is the same thing as a monoid. The morphisms are the elements of the monoid, and composition is multiplication.

So, we can also view \mathbb{R} as a **category** with only one object, with $\circ = +$.

Each operation $\bar{\mathbf{p}}$ preserves addition. So $\bar{\mathbf{p}}$ is a **functor** $\mathbb{R}^n \rightarrow \mathbb{R}$.

It follows that \mathbb{R} , as a one-object category, is a categorical Δ -algebra.

Maps between categorical algebras for an operad

Fix an operad P and categorical P -algebras \mathbf{B} and \mathbf{A} .

A **lax map** $\mathbf{B} \rightarrow \mathbf{A}$ is a functor $G: \mathbf{B} \rightarrow \mathbf{A}$ together with a natural transformation

$$\begin{array}{ccc} \mathbf{B}^n & \xrightarrow{G^n} & \mathbf{A}^n \\ \bar{\theta} \downarrow & \swarrow \gamma_\theta & \downarrow \bar{\theta} \\ \mathbf{B} & \xrightarrow{G} & \mathbf{A} \end{array}$$

for each $n \geq 0$ and $\theta \in P_n$, satisfying axioms.

Explicitly: it's a functor G together with a map

$$\gamma_{\theta, b^1, \dots, b^n}: \bar{\theta}(Gb^1, \dots, Gb^n) \rightarrow G(\bar{\theta}(b^1, \dots, b^n))$$

for each $\theta \in P_n$ and $b^1, \dots, b^n \in \mathbf{B}$, satisfying naturality and axioms on:

- (i) composition,
- (ii) identity.

4. *Internal algebras*

Internal algebras in a categorical algebra for an operad

Fix an operad P and a categorical P -algebra \mathbf{A} .

Write $\mathbf{1}$ for the categorical P -algebra with one object and only the identity morphism. (This category is a categorical P -algebra in a unique way.)

Definition: An **internal algebra** in \mathbf{A} is a lax map $\mathbf{1} \rightarrow \mathbf{A}$.

Explicitly: it's an object $a \in \mathbf{A}$ together with a map

$$\gamma_\theta: \bar{\theta}(a, \dots, a) \rightarrow a$$

for each $n \geq 0$ and $\theta \in P_n$, satisfying axioms on

- (i) composition, (ii) identity.

Examples:

- Let P be the terminal operad. Let \mathbf{A} be a strict monoidal category. An internal P -algebra in \mathbf{A} is just a monoid in \mathbf{A} .
- Let $P = P^M$. Let \mathbf{A} be a category with an M -action. An internal P^M -algebra in \mathbf{A} is an object $a \in \mathbf{A}$ with a map $\gamma_m: m \cdot a \rightarrow a$ for each $m \in M$, satisfying action-like axioms.

Internal algebras in a one-object categorical algebra

Fix an operad P and a categorical P -algebra \mathbf{A} .

We just saw: an internal P -algebra in \mathbf{A} is an object $a \in \mathbf{A}$ with a map

$$\gamma_\theta: \bar{\theta}(a, \dots, a) \rightarrow a$$

for each $n \geq 0$ and $\theta \in P_n$, satisfying axioms.

What if \mathbf{A} has only one object?

That is, what if \mathbf{A} is a monoid A ?

An internal algebra in the one-object category corresponding to A is a sequence of functions

$$(\gamma: P_n \rightarrow A)_{n \geq 0},$$

satisfying axioms on

- (i) composition,
- (ii) identity.

Topologizing everything

Everything so far can be done in the world of topological spaces instead of sets.

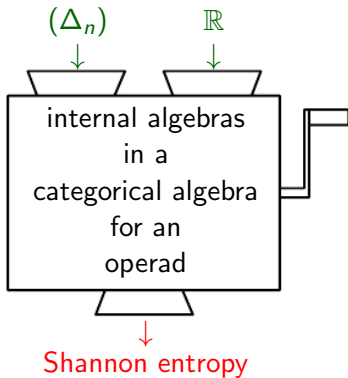
(Jargon: we work *internally* to the category **Top** instead of **Set**.)

Explicitly, this means that throughout, we add a condition

(iii) continuity

to the conditions (i) and (ii) that appear repeatedly.

*5. The theorem: how entropy
arises*



The theorem

Recall We have:

- the (topological) operad $\Delta = (\Delta_n)_{n \geq 0}$ of simplices
- the one-object (topological) category \mathbb{R} : morphisms are real numbers, $\circ = +$
- the one-object (topological) categorical Δ -algebra \mathbb{R} .

Recall For an operad P , an internal algebra in a one-object categorical P -algebra A is a sequence of functions $(P_n \rightarrow A)_{n \geq 0}$, satisfying axioms.

So, an internal algebra in the categorical Δ -algebra \mathbb{R} is a sequence of functions $(\Delta_n \rightarrow \mathbb{R})_{n \geq 0}$, satisfying axioms.

One famous sequence of functions $(\Delta_n \rightarrow \mathbb{R})_{n \geq 0}$ is Shannon entropy:

$$H : \mathbf{p} \mapsto - \sum p_i \log p_i.$$

Theorem

The internal algebras in the categorical Δ -algebra \mathbb{R} are precisely the scalar multiples of Shannon entropy.

The theorem

Theorem

The internal algebras in the categorical Δ -algebra \mathbb{R} are precisely the scalar multiples of Shannon entropy.

Explicit version of the theorem (no categorical jargon)

Take a sequence of functions $(\gamma: \Delta_n \rightarrow \mathbb{R})_{n \geq 0}$.

Then $\gamma = cH$ for some $c \in \mathbb{R}$ if and only if γ satisfies:

- (i) **composition:** $\gamma(\mathbf{p} \circ (\mathbf{q}_1, \dots, \mathbf{q}_n)) = \gamma(\mathbf{p}) + \sum_i p_i \gamma(\mathbf{q}_i)$
- (ii) **identity:** $\gamma((1)) = 0$
- (iii) **continuity:** each function γ is continuous.

Proof: This explicit form is almost equivalent to a 1956 theorem of Faddeev, except that he imposed a symmetry axiom that turns out to be redundant. \square

Summary

We have met various very general concepts:

- operads (a cousin of clones/algebraic theories)
- algebras for an operad: both set-based and categorical algebras
- internal algebras in a categorical algebra for an operad.

The simplest example:

- for the terminal operad ($P_n = \{*_n\}$ for all n),
a categorical algebra is a strict monoidal category \mathcal{M} ,
and the internal algebras in \mathcal{M} are the monoids in \mathcal{M} .

Another fundamental example:

- for the operad of simplices $(\Delta_n)_{n \geq 0}$,
one categorical algebra is the one-object category $(\mathbb{R}, +)$,
and the internal algebras in it are the multiples of Shannon entropy.

In short:

Entropy is inevitable.

Preview of Thursday

On Thursday...

We will follow this algebraic, axiomatic approach to entropy and use it to do something new, involving:

- “probabilities” that are not real numbers but integers modulo a prime
- an answer to the question: why is it reasonable to say that

$$\log \sqrt{8} \equiv 3 \pmod{7}?$$