Charles University Prague – Department of Algebra

Disorder in Algebra

Joint work with David Stanovský

Filippo Spaggiari
spaggiari@karlin.mff.cuni.cz

AAA 105 – Prague, Czech Republic
May 31th – June 2nd, 2024

Outline

1. Algebraic Structures
2. Information Theory
3. Entropy and Universal Algebra
4. Entropy Lower Bounds

1. Algebraic Structures

Definition (**Multiplication Maps**)

Let $X = (X, \triangleright)$ be a binary algebraic structure, and let $a \in X$. We define

- The **left multiplication map** by a as $\mathsf{L}_a : x \mapsto a \triangleright x$.
- The **right multiplication map** by a as $\mathsf{R}_a : x \mapsto x \triangleright a$.

Definition (**Left Quasigroup**)

The binar $X = (X, \triangleright)$ is called **left quasigroup** if all left multiplication maps L_a are permutations. For a left quasigroup X we define the **left multiplication group** as

$$\mathsf{LMlt}(X) = \langle\, \mathsf{L}_a : \ a \in X \,\rangle \leq \mathsf{Sym}(X).$$

Definition (**Rack and Quandle**)

The binar $X = (X, \triangleright)$ is called **rack** if all left multiplication maps L_a are automorphisms. For a rack X we define the **left multiplication group** as

$$\mathsf{LMlt}(X) = \langle\, \mathsf{L}_a : \, a \in X \,\rangle \leq \mathsf{Aut}(X).$$

If $\mathsf{L}_a(a) = a$ for all $a \in X$, the rack X is called **quandle**.

X	**binar**	**left quasigroup**	**rack**	**quandle**
L_a	nothing special	permutations	automorphisms	aut. fixing a point

Remark. Quandle axioms encode the movement of *knots* in the very same way that group axioms encode the symmetry of figures.

Example (**Projection Quandle**)

The structure $(X, x \triangleright y = y)$ is a **projection quandle**.

$\triangleright$	1	2	3	4	5
1	1	2	3	4	5
2	1	2	3	4	5
3	1	2	3	4	5
4	1	2	3	4	5
5	1	2	3	4	5

Example (**Dihedral Quandle**)

The structure $R_n = (\mathbb{Z}_n, x \triangleright y = 2x - y)$ is a **dihedral quandle**.

2. Information Theory

Entropy of a Discrete Distribution

Definition (Discrete Probability Distribution)

A **discrete probability distribution (DPD)** over a finite set X is a sequence $p = (p_x \colon x \in X)$ such that

- $0 \leq p_x \leq 1$ for every $x \in X$.
- $\sum_{x \in X} p_x = 1$.

Definition (Entropy of a DPD)

The **entropy** of p is the value

$$\mathsf{h}(p) = -\sum_{x \in X} p_x \log(p_x).$$

Definition (**Entropy of a Function**)

Let $f : X \to X$ be a function. We define the **distribution** of f as

$$\hat{f} = \left(\frac{|f^{-1}(x)|}{|X|} : x \in X \right).$$

Consequently, the **entropy** of f is $\mathsf{h}(f) = \mathsf{h}(\hat{f})$.

Proposition (**Properties of** h)

Let $f : X \to X$ be a function. Then

1. $0 \leq \mathsf{h}(f) \leq \log |X|$.
2. $\mathsf{h}(f) = 0$ *if and only if f is constant.*
3. $\mathsf{h}(f) = \log |X|$ *if and only if f is a permutation.*

Definition (Entropy of a Left Quasigroup)

Let X be a finite left quasigroup. We define the **entropy** of X as

$$\mathsf{H}(X) = \frac{1}{|X|} \sum_{x \in X} \mathsf{h}(\mathsf{R}_x).$$

Proposition (Properties of H)

Let X be a finite left quasigroup. Then

1. $0 \leq \mathsf{H}(X) \leq \log |X|$.
2. $\mathsf{H}(X) = 0$ *if and only if X is a projection.*
3. $\mathsf{H}(X) = \log |X|$ *if and only if X is a Latin square.*

$\triangleright$	1	2	3	4	5
1	1	2	3	4	5
2	1	2	3	4	5
3	1	2	3	4	5
4	1	2	3	4	5
5	1	2	3	4	5

Projection

Entropy = 0
Min disorder
Max predictability

$\triangleright$	1	2	3	4	5
1	1	5	4	3	2
2	3	2	1	5	4
3	5	4	3	2	1
4	2	1	5	4	3
5	4	3	2	1	5

Latin Square

Entropy = $\log |X|$
Max disorder
Min predictability

Remark. The entropy of a left quasigroup measures its deviation from projection to Latin square: it indicates how *disordered* and *unpredictable* its table is.

Computation of Entropy

Example (Entropy of Dihedral Quandle)

Let $R_n = (\mathbb{Z}_n, x \triangleright y = 2x - y)$ be a dihedral quandle. Then

$$\mathsf{H}(X) = \left\langle \begin{array}{ll} \log(n) & n \text{ odd} \\ \frac{1}{2}\log(n) & n \text{ even} \end{array} \right.$$

R_5	1	2	3	4	5
1	1	3	5	2	4
2	5	2	4	1	3
3	4	1	3	5	2
4	3	5	2	4	1
5	2	4	1	3	5

R_6	1	2	3	4	5	6
1	1	6	5	4	3	2
2	3	2	1	6	5	4
3	5	4	3	2	1	6
4	1	6	5	4	3	2
5	3	2	1	6	5	4
6	5	4	3	2	1	6

3. Entropy and Universal Algebra

Proposition (**Entropy of the Product**)

Let X and Y be finite left quasigroups. Then

$$\mathsf{H}(X \times Y) = \mathsf{H}(X) + \mathsf{H}(Y).$$

Proposition (**Entropy of the Quotient**)

Let X be a finite left quasigroup, and let θ be a uniform congruence on X. Then

$$\mathsf{H}(X/\theta) \leq \mathsf{H}(X).$$

Proposition (Entropy of the Substructures)

Let $Y \leq X$ be finite left quasigroups. Then

$$\mathrm{H}(Y) \leq \mathrm{H}(X).$$

FALSE

Remark. Not so fast...

Example (**Entropy of Substructures**)

There are left quasigroups $S \leq R$ such that

$$|R| = 21, \qquad |S| = 15, \qquad \mathsf{H}(R) \approx 1.78848, \qquad \mathsf{H}(S) \approx 1.79996.$$

Moreover, R and S are *connected quandles*, and they are the smallest counterexample in this class.

Proposition (**Entropy of Substructures – The best we can do**)

Let $Y \leq X$ be finite left quasigroups. Then

$$\mathsf{H}(Y) \leq \frac{|X|^2}{|Y|^2}\mathsf{H}(X).$$

Disjoint Sum

Definition (Disjoint Sum)

Let X and Y be left quasigroups. The **disjoint sum** $X \# Y$ is the left quasigroup structure defined on the disjoint union $X \sqcup Y$ by

$$x \triangleright y = \begin{cases} x \triangleright^X y & \text{if } x, y \in X \\ x \triangleright^Y y & \text{if } x, y \in Y \\ y & \text{otherwise.} \end{cases}$$

For an integer $k \geq 1$ we denote by $kX = X \# X \# \dots \# X$ (k times).

$X \# Y$	X	Y
X	X	proj.
Y	proj.	Y

kX	X	X	X
X	X	proj.	proj.
X	proj.	X	proj.
X	proj.	proj.	X

Entropy of the Disjoint Multiple

Proposition (Entropy of the Disjoint Multiple)

Let X be a finite left quasigroup, and let $k \geq 1$ be an integer. Then

$$\mathsf{H}(kX) \leq \frac{1}{k}\mathsf{H}(X) + \left(\log k - \frac{k-1}{k}\log(k-1)\right).$$

Corollary (Entropy Limit of the Disjoint Multiple)

Let X be a finite left quasigroup. Then

$$\lim_{k\to\infty} \mathsf{H}(kX) = 0.$$

Remark. We have arbitrarily large left quasigroup with arbitrarily small entropy.

4. Entropy Lower Bounds

(for Quandles)

Connectedness

Definition (Connected Quandle)

A finite quandle Q is **connected** if the natural action of $\mathsf{LMlt}(Q)$ on Q is transitive.

Proposition

Let Q be a finite connected quandle. Then $\mathsf{H}(Q) = \mathsf{h}(\mathsf{R}_x)$ for every $x \in Q$.

Remark. Connectedness *pushes* towards disorder.

Proposition (Lower Bound for Connected Quandles)

There is no entropy lower bound for the class of connected quandles.

Definition (Faithful Quandle)

A finite quandle Q is **faithful** if $\mathsf{L}_x \neq \mathsf{L}_y$ whenever $x \neq y$.

Remark. Faithfulness *pushes* towards disorder.

Proposition (Lower Bound for Faithful Quandles)

There is no entropy lower bound for the class of faithful quandles.

Proof idea. Disjoint sum of faithful structures is faithful.

Proposition (Lower Bound for CFNL Quandles)

There is no entropy lower bound in the class of connected faithful (non-Latin) left quasigroups.

Proof. The conjugacy class of $(1\,2)$ in S_n is a quandle with respect to the conjugation operation $(\mathrm{Cl}_{S_n}((1\,2)), x \triangleright y = xyx^{-1})$. Because an increasing number of transpositions conjugate $(1\,2)$ to itself as n grows, the entropy is very low.

Conclusions

Summary

- We developed a tool to analyze and describe the state of disorder and predictability of an algebraic structure.
- The entropy function performs well with respect to Universal Algebraic constructions.

New horizons

- Is it possible to prove any significant theorems using constraints on the entropy?
- Are there any structural properties that arise as sufficient conditions based solely on high or low values of entropy?
- Is there a structural property, other than Latinness, that defines a class of structures with a lower bound on entropy?

[1] **T. M. Cover**, ***Elements of information theory***, **John Wiley & Sons, 1999.**

Thank you for your attention!

spaggiari@karlin.mff.cuni.cz