Algebraic and other entropies

Antongiulio Fornasiero
antongiulio.fornasiero@gmail.com

HUJI

AILA 2017

Introduction

Joint work with D. Dikranjan and A. Giordano Bruno

A short introduction to algebraic entropy,
with particular emphasis on the Addition Theorem.

- Algebraic entropy has several variants (ent, h_{rk}, h_{alg}, $\widetilde{\mathrm{ent}}$, ...)
- Introduced (for one endomorphism) in [Adler, Kohnheim, McAndrew '65] and [Weiss '75], became popular after [Dikranjan, Goldsmith, Salce, Zanardo '09]
- Inspired by similar notions in:
  - information theory (Shannon),
  - ergodic theory (Kolmogorov and Sinai),
  - topological dynamics (Peters and Weiss)
- We will consider dynamical entropies (i.e.: entropies of endomorphisms)

Contents

Algebraic entropy of one endomorphism

- B Abelian group
- ϕ endomorphism of B
- $\ell(B) := \log|B|$

Definition (Entropy)

$$H_\ell(\phi, B_0) := \lim_{n\to\infty} \frac{\ell(\sum_{i=0}^{n-1} \phi^i(B_0))}{n}$$
$$\mathrm{ent}(\phi) := \sup\Big\{ H_\ell(\phi, B_0) : B_0 < B \text{ finite subgroup}\Big\}.$$

The subgroup $\sum_{i=0}^{n-1} \phi^i(B_0)$ is the partial trajectory of B_0 under ϕ.
$H_\ell(\phi, B_0)$ is the average growth of ℓ along the partial trajectory of B_0.
The limit in the definition of H_ℓ exists (Fekete's Lemma).

Basic properties

- ℓ is additive: if $0 \to A \to B \to C \to 0$ is an exact sequence of (Abelian) groups,
$$\ell(B) = \ell(A) + \ell(C)$$
- An Abelian group B with an endomorphism ϕ is the same object as a $\mathbb{Z}[X]$-module ($X * b = \phi(b)$)
- ent behaves as a "rank" function on $\mathbb{Z}[X]$-modules (more precisely, it is a length function for torsion $\mathbb{Z}[X]$-modules)
- $\mathrm{ent}(\phi)$ depends only on the restriction of ϕ to the torsion of B (since every finite group is torsion)
- Two isomorphic $\mathbb{Z}[X]$-modules have the same entropy (ent is an invariant)
- If ϕ is an automorphism, then $\mathrm{ent}(\phi) = \mathrm{ent}(\phi^{-1})$.

Amenable (semi-)groups

G cancellative semi-group.
G is right amenable if it there exists a Følner net $(F_i)_{i\in I}$ for G: each F_i is a nonempty subset of G,

$$\forall g \in G \ \lim_{i\to\infty} \frac{|F_i g \,\Delta\, F_i|}{|F_i|} = 0.$$

Equivalently, if it exists a nonempty *-finite set $F \subset {}^*G$ (in the non-standard universe) such that

$$\forall g \in G \quad \frac{|Fg \,\Delta\, F|}{|F|} \text{ is infinitesimal}$$

(Notice that g varies only among standard elements)

Notes

- Every Abelian (cancellative semi-)group is amenable.
- If $G = \mathbb{Z}$ or $G = \mathbb{N}$, take $F_n := [0, n)$.
- If G is countable, we can find Følner sequences: otherwise, a net may be necessary.
- The free group in 2 generators, and any group containing it, is not amenable.
- Right amenable groups are also left amenable;
the same is not true for cancellative semi-groups.
- Here by "amenable group" we mean "discrete amenable group": there is a definition of amenability also for topological groups.
- There are many equivalent definitions of amenability: invariant mean, invariant measure, ...

Algebraic entropy of a (semi-)group action

- B Abelian group
- G right-amenable cancellative semi-group
- α left action of G on B by group endomorphisms.

Definition (Entropy)

$$F * B_0 := \sum_{g \in F} \alpha(g)(B_0), \qquad \text{the partial trajectory}$$

$$H_\ell(\alpha, B_0) := \lim_{i \to \infty} \frac{\ell(F_i * B_0)}{|F_i|}$$

$$\mathrm{ent}(\alpha) := \sup\Big\{ H_\ell(\alpha, B_0) : B_0 < B \text{ finite subgroup} \Big\}.$$

Notes

- The limit in the definition of H_ℓ exists and is independent from the choice of the Følner net:
  [Ornstein, Weiss] for the case when G is a group,
  [Ceccherini-Silberstein, Krieger, Coornaert '12] for cancellative semigroups.
- Taking $G = \mathbb{N}$ and $F_n := [0, n)$, we recover the definition of entropy for one endomorphism.
- Using non-standard analysis, one can define

$$H_\ell(\alpha, B_0) := st\Big(\frac{\ell(F * B_0)}{|F|}\Big),$$

where F is a *-finite almost invariant subset of $^*G$.

Basic properties

- An Abelian group B with an action of a semigroup G is the same object as a $\mathbb{Z}[G]$-module ($g * b = \alpha(g)(b)$)
- ent behaves as a "rank" function on $\mathbb{Z}[G]$-modules (more precisely, it is a length function for torsion $\mathbb{Z}[G]$-modules)
- $\mathrm{ent}(\alpha)$ depends only on the action on the torsion of B
- Two isomorphic $\mathbb{Z}[G]$-modules have the same entropy (ent is an invariant)
- If G is commutative group, then α^{-1} is also a left action, and $\mathrm{ent}(\alpha^{-1}) = \mathrm{ent}(\alpha)$.
- $h_{top}(G \curvearrowright \hat{A}) = \mathrm{ent}(G \curvearrowright A)$, where $\hat{A}$ is the Pontryagin dual

The Addition Theorem for algebraic entropy

Statement

- G is a right-amenable cancellative semigroup
- B is an Abelian group
- α is a (left) action of G on B (by group endomorphisms)
- A is an α-invariant subgroup of B (for every $g \in G$, $g * A \subseteq A$)
- α_A is the induced action of G on A
- $\alpha_{B/A}$ is the induced action of G on B/A.

Theorem (Addition Theorem)

If B is a torsion group, then

$$\mathrm{ent}(\alpha) = \mathrm{ent}(\alpha_A) + \mathrm{ent}(\alpha_{B/A}).$$

Notes

AT was already known for a single endomorphism:
see [Dikranjan, Goldsmith, Salce, Zanardo ’09] and its generalization in [Salce, Virili ’15]

Theorem (AT: equivalent formulation)

If $$0 \to A \to B \to C \to 0$$ *is an exact sequence of torsion* $\mathbb{Z}[G]$*-modules, then*

$$\operatorname{ent}(B) = \operatorname{ent}(A) + \operatorname{ent}(C).$$

The assumption in AT that B is torsion is necessary: there are easy examples when the conclusion fails for non-torsion groups.

Example

Let $B := \mathbb{Z}[X]$ as $\mathbb{Z}[X]$-module. Let $A := 2B$.
Then, B and A are torsion-free, and therefore $\operatorname{ent}(B) = \operatorname{ent}(A) = 0$, while $\operatorname{ent}(B/A) = \log 2$.

Notes

$\mathbb{Z}[X]$ is the Bernoulli shift on the group $\mathbb{Z}$,
and similarly $\mathbb{Z}/2\mathbb{Z}[X]$ is the Bernoulli shift on the group $\mathbb{Z}/2\mathbb{Z}$

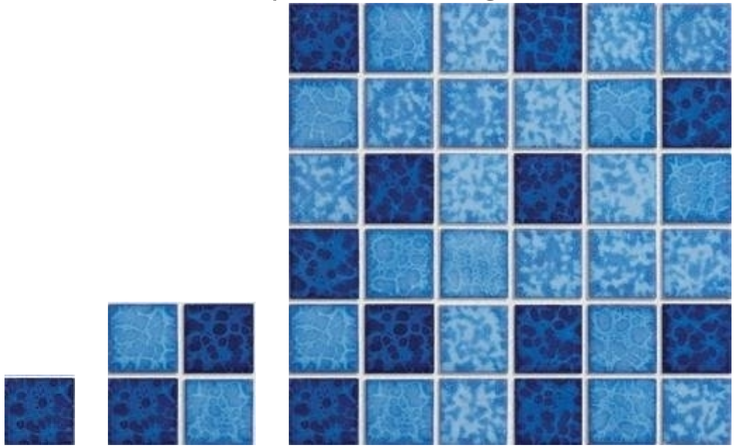
Idea of proof

We will give an idea of the proof of the Addition Theorem under a simplifying assumption
(which include the cases when $G = \mathbb{Z}$ or $G = \mathbb{N}$).
We will assume the following:

Monotiling condition

- G is countable;
- There exists a Følner sequence $(F_n)_{n\in\mathbb{N}}$ for G such that $1 \in F_n$ and each F_n tiles F_{n+1}:
  that is, F_{n+1} is the disjoint union of translates of F_n.

For instance, $\mathbb{N}$ and $\mathbb{Z}$ satisfy the monotiling condition: $F_n := [0, n!)$.
$\mathbb{N}^2$ and $\mathbb{Z}^2$ also satisfy the monotiling condition.



Exercise

$\mathbb{Q}$ satisfies the monotiling condition.

Notes

- Every countable locally finite group is amenable and satisfies the monotiling condition.
- A variant of the monotiling condition was studied in [Ornstein, Weiss '87]
- The fundamental ingredient in the proof of AT in the general case is Ornstein-Weiss Lemma, which proves that every amenable group satisfies some version of tiling.
- Ornstein-Weiss Lemma has been extended to right amenable cancelaltive semi-groups by [Ceccherini-Silberstein, Krieger, Coornaert '12]

The proof

Main step

Notation: $\ell(X \mid Y) := \log\left|(X+Y)/Y\right|$.

Remark

For every A_0, A_1, B_0, B_1 finite subgroups of B,

$$\ell(B_0 + B_1 \mid A_0 + A_1) \leq \ell(B_0 \mid A_0) + \ell(B_1 \mid A_1)$$

Corollary

$\forall n \geq M$, $F_n = \bigsqcup_{g \in D} g \cdot F_M$ for some finite $D \subseteq G$:

$$\frac{\ell(F_n * B_0 \mid F_n * A_0)}{|F_n|} \leq \frac{\sum_{g \in D} \ell(g * F_M * B_0 \mid g * F_M * A_0)}{|F_n|} \leq$$

$$\leq \frac{|D|\,\ell(F_M * B_0 \mid F_M * A_0)}{|D|\,|F_M|} = \frac{\ell(F_M * B_0 \mid F_M * A_0)}{|F_M|}$$

Notes

- The main properties of the function ℓ are that it is positive, submodular, and additive (on the family of finite subgroups of B)

$$\begin{cases} \ell \geq 0 \\ \ell(A+B \mid C) = \ell(A \mid B+C) + \ell(B \mid C) \\ \ell(A \mid B) \text{ is increasing in } A \text{ and decreasing in } B \end{cases}$$

- For the Corollary, we are assuming that (F_n) is a Følner sequence for G witnessing the mono-tiling condition.

The only difficult part of AT is proving that

$$\mathrm{ent}(\alpha) \leq \mathrm{ent}(\alpha_A) + \mathrm{ent}(\alpha_{B/A}).$$

(The opposite inequality is easy, and is the only place where the assumption that B is torsion is used).
Let $B_0 < B$ be a finite subgroup and $C_0 := \pi(B_0) < B/A$. Fix $\varepsilon > 0$.
Choose M such that, for every $n \geq M$,

$$H(\alpha; B_0) \simeq_\varepsilon \frac{\ell(F_n * B_0)}{|F_n|}$$
$$H(\alpha_{B/A}; C_0) \simeq_\varepsilon \frac{\ell(F_n * B_0 \mid A)}{|F_n|}$$

Let $A_0 := (F_M * B_0) \cap A$.
We have the exact sequence of Abelian groups

$$0 \to A_0 \to F_M * B_0 \to F_M * C_0 \to 0.$$

Notes

1. The above sequence is exact only at M: this is the main difficulty
2. We use the notation $r \simeq_\varepsilon s$ if $|r - s| < \varepsilon$.
3. $\pi : B \to B/A$ is the canonical projection.

Let $n > M$.

$$\frac{\ell(F_n * B_0 \mid F_n * A_0)}{|F_n|} \leq \frac{\ell(F_M * B_0 \mid F_M * A_0)}{|F_M|} \simeq_\varepsilon H(\alpha_{B/A}, C_0) \leq \mathrm{ent}(\alpha_{B/A})$$

If we choose $n > M$ large enough:

$$\frac{\ell(F_n * A_0)}{|F_n|} \simeq_\varepsilon H(\alpha_A, A_0) \leq \mathrm{ent}(\alpha_A).$$

Therefore,

$$H(\alpha, B_0) \simeq_\varepsilon \frac{\ell(F_n * B_0)}{|F_n|} \leq \frac{\ell(F_n * B_0 \mid F_n * A_0)}{|F_n|} + \frac{\ell(F_n * A_0)}{|F_n|} \leq$$

$$\leq 2\varepsilon + \mathrm{ent}(\alpha_{B/A}) + \mathrm{ent}(\alpha_A)$$

The above holds for every $\varepsilon > 0$ and every B_0 finite subgroup of B:

$$\mathrm{ent}(\alpha) \leq \mathrm{ent}(\alpha_{B/A}) + \mathrm{ent}(\alpha_A) \quad \square$$

Notes

The proof of AT used very few properties of Abelian groups and of the function ℓ; the same proof can be used for other entropies.
The function ℓ will change in the various situations.
For instance, for Kolmogorov-Sinai entropy, the rôle of ℓ is taken by Shannon entropy $H(\cdot \mid \cdot)$.

Rank entropy

Definition

R integral domain, with field of fraction R_0
rk_R rank function on R-modules: $\mathrm{rk}_R(B) = \dim_{R_0}(B \otimes_R R_0)$,

$$\mathrm{rk}_R(B \mid A) := \mathrm{rk}_R((A+B)/A).$$

G amenable (cancellative semi-)group with Følner net $(F_i)_{i \in I}$;
α action of G on R-module B.

Entropy: $H_{\mathrm{rk}_R}(\alpha, B_0) := \lim_{i \to \infty} \frac{\mathrm{rk}_R(F_i * B_0)}{|F_i|}$

$$h_{\mathrm{rk}_R}(\alpha) := \sup\left\{ H_{\mathrm{rk}_R}(\alpha, B_0) : B_0 < B, \mathrm{rk}_R(B) < \infty \right\}$$

h_{rk_R} satisfies AT.

Example

Let $G = \mathbb{N}$ and B be an $R[X]$-module. Then,

$$h_{\mathrm{rk}_R}(B) = \mathrm{rk}_{R[X]}(B)$$

Dynamical entropy of matroids

(X, rk) finitary matroid/pregeometry
($\mathrm{rk} : \mathcal{P}(X) \to \mathbb{N} \cup \{\infty\}$ is the rank function)
α action of a group G on (X, r)

Example

X field, $\mathrm{rk}(\bar{a}) := \mathrm{tr.deg.}(\bar{a})$, G groups of field automorphisms of X.

Definition (Entropy)

$$H_{\mathrm{rk}}(\alpha, \bar{b}) := \lim_{i \to \infty} \frac{\mathrm{rk}\left(\bigcup_{g \in F_i} g * \bar{b}\right)}{|F_i|}$$

$$h_{\mathrm{rk}}(\alpha) := \sup\left\{ H_{\mathrm{rk}}(\alpha, \bar{b}) : \bar{b} \subseteq X, \bar{b} \text{ finite} \right\}$$

Lemma

If $G = \mathbb{Z}^m$, then h_{rk} is a matroid on X.

Notes

The only difficulty is the analogue of AT for h_{rk}

Example

K field, σ field automorphism.
"Closure operator for h_{rk}" = "differential-algebraic closure"
$x \in cl^{\sigma}(A)$ iff there exists a differential-algebraic polynomial $f(X) := p(X, X^{\sigma}, X^{\sigma^2}, \dots)$
with coefficients in the field generated by $A \cup \sigma(A) \cup \sigma^2(A) \cup \dots$
such that $f(x) = 0$.

When $K \models ACFA$,

$$U(\bar{a}) = h_{\mathrm{rk}}(\bar{a}) \cdot \omega + \mathrm{o}(\omega)$$

Notes

- Riečan's entropy is a "Kolmogorov-Sinai entropy for fuzzy sets"
- A different construction of dynamical entropy for MV-algebrae with product is in [Petrovičová '01]
- Dynamical quantum entropy definition is also based on partitions of unity.
- There is also a connection between algorithmic complexity and entropy: for a fixed Bernoulli process, the average-case growth rate of the algorithmic complexity of a string is equal to the Shannon entropy of the source (up to a multiplicative constant).

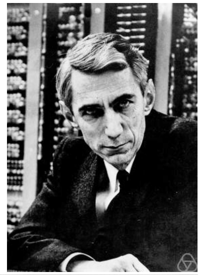
Dynamical entropy of MV-algebrae

Let A be a lattice-ordered Abelian group, and $0 < u \in A$.
The interval $[0, u]$ (with suitable operations induced by the ones on A) is an MV-algebra (and every such MV-algebra can be represented this way [Mundici '86]).
Let $m : A \to \mathbb{R}$ be a homomorphism of ordered groups, with $m(u) = 1$. Let $\phi : A \to A$ be an automorphism preserving m.

Example

(X, μ) probability space, $A := \ell^{\infty}(X)$, $u = 1$, $m(f) := \int_X f \, \mathrm{d}\mu$.

[Riečan '05] defined the entropy of ϕ (w.r.t. m), using partitions of unity in $[0, u]$.
His definition can be extended to actions of amenable groups on A.



> *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, nobody knows what entropy really is, so in a debate you will always have the advantage."*

Claude Shannon