Entropy, Mahler Measure and Bernoulli Convolutions

Emmanuel Breuillard (joint with Péter Varjú)

Analysis and Beyond, celebrating Jean Bourgain, IAS Princeton, May 24th, 2016

Group growth

G a group.

$S = \{1, s_1^{\pm 1}, \ldots, s_k^{\pm 1}\}$ a finite symmetric generating set.

S^n denotes the n-th fold product set $S^n := S \cdot \ldots \cdot S$

How does the cardinality of S^n grow with n ?

Growth of matrix groups

Suppose $G = \mathrm{GL}_d(\mathbb{C})$, and $S \subset \mathrm{GL}_d(\mathbb{C})$
We denote the rate of exponential growth by

$$\rho(S) := \lim_{n \to +\infty} |S^n|^{1/n}$$

Growth of matrix groups

Suppose $G = \mathrm{GL}_d(\mathbb{C})$, and $S \subset \mathrm{GL}_d(\mathbb{C})$
We denote the rate of exponential growth by

$$\rho(S) := \lim_{n \to +\infty} |S^n|^{1/n}$$

G is said to have exponential growth if $\rho(S) > 1$ (this is independent of the choice of S).

Growth of matrix groups

Suppose $G = \mathrm{GL}_d(\mathbb{C})$, and $S \subset G$.

We denote the rate of exponential growth by

$$\rho(S) := \lim_{n \to +\infty} |S^n|^{1/n}$$

Growth of matrix groups

Suppose $G = \mathrm{GL}_d(\mathbb{C})$, and $S \subset G$.

We denote the rate of exponential growth by

$$\rho(S) := \lim_{n \to +\infty} |S^n|^{1/n}$$

G is said to have exponential growth if $\rho(S) > 1$ (this is independent of the choice of S).

Growth of matrix groups

Suppose $G = \mathrm{GL}_d(\mathbb{C})$, and $S \subset G$.

We denote the rate of exponential growth by

$$\rho(S) := \lim_{n \to +\infty} |S^n|^{1/n}$$

G is said to have exponential growth if $\rho(S) > 1$ (this is independent of the choice of S).

Let $Upp_d(\mathbb{C}) \leqslant \mathrm{GL}_d(\mathbb{C})$ be the unipotent upper triangular subgroup:

$$Upp_d(\mathbb{C}) = \{g \in \mathrm{GL}_d(\mathbb{C}); g_{ii} = 1, g_{ij} = 0 \text{ if } i > j\}.$$

Easy fact: if $S \subset Upp_d(\mathbb{C})$ then $|S^n| = O(n^{O(1)})$.

Growth of matrix groups

Theorem (Tits 1972)

For $S \subset \mathrm{GL}_d(\mathbb{C})$, the following are equivalent:

1. $\rho(S) = 1$
2. $\exists C > 0$ *s.t.* $|S^n| = O(n^C)$,
3. *the finite index subgroup of* $\langle S \rangle$ *is isomorphic to a subgroup of* $\mathrm{Upp}_d(\mathbb{C})$.

$\longrightarrow$ a consequence of the Tits alternative and its proof.

Uniform growth

How does $\rho(S)$ depend on S ?

Uniform growth

How does $\rho(S)$ depend on S ?

Gromov's question: fix $\Gamma = \langle S \rangle$, vary S among generating subsets, is $\rho(S)$ bounded away from 1 ?

Uniform growth

How does $\rho(S)$ depend on S ?

Gromov's question: fix $\Gamma = \langle S \rangle$, vary S among generating subsets, is $\rho(S)$ bounded away from 1 ?

Eskin-Mozes-Oh 2001 : answered this affirmatively for $\Gamma \leqslant GL_d(\mathbb{C})$, by showing that unless $\rho(S) = 1$, $\exists N = N(\Gamma) \in \mathbb{N}$ s.t. for all generating subsets S of Γ, S^N contains generators a, b of a free sub-semigroup. Thus:

$$\forall n, |S^{Nn}| \geqslant 2^n \longrightarrow \rho(S) \geqslant 2^{\frac{1}{N}}.$$

Uniform growth

How does $\rho(S)$ depend on S ?

Gromov's question: fix $\Gamma = \langle S \rangle$, vary S among generating subsets, is $\rho(S)$ bounded away from 1 ?

Eskin-Mozes-Oh 2001 : answered this affirmatively for $\Gamma \leqslant \mathrm{GL}_d(\mathbb{C})$, by showing that unless $\rho(S) = 1$, $\exists N = N(\Gamma) \in \mathbb{N}$ s.t. for all generating subsets S of Γ, S^N contains generators a, b of a free sub-semigroup. Thus:

$$\forall n, |S^{Nn}| \geqslant 2^n \longrightarrow \rho(S) \geqslant 2^{\frac{1}{N}}.$$

B.+Gelander 2005: improved this showing the we can get the *subgroup* $\langle a, b \rangle$ to be free.

Uniform growth conjecture

Conjecture (Uniform growth conjecture)

Given $d \in \mathbb{N}$, *there is* $\varepsilon(d) > 0$ *such that for every finite symmetric* $S \subset \mathrm{GL}_d(\mathbb{C})$,

- *either* $\rho(S) = 1$
- *or* $\rho(S) > 1 + \varepsilon$.

Uniform growth conjecture

Conjecture (Uniform growth conjecture)

Given $d \in \mathbb{N}$*, there is* $\varepsilon(d) > 0$ *such that for every finite symmetric* $S \subset \mathrm{GL}_d(\mathbb{C})$,

- *either* $\rho(S) = 1$
- *or* $\rho(S) > 1 + \varepsilon$.

A example in the affine group

For $\lambda \in \mathbb{C}^\times$, let

$$S_\lambda := \{1, \begin{pmatrix} \lambda & 1 \\ 0 & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} \lambda & -1 \\ 0 & 1 \end{pmatrix}^{\pm 1}\} \subset \mathrm{GL}_2$$

- S_λ generates a group of affine transformations of $\mathbb{C}$, $x \mapsto \lambda x + 1$ and $x \mapsto \lambda x - 1$.
- it has polynomial growth iff λ is a root of unity.

A example in the affine group

For $\lambda \in \mathbb{C}^\times$, let

$$S_\lambda := \{1, \begin{pmatrix} \lambda & 1 \\ 0 & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} \lambda & -1 \\ 0 & 1 \end{pmatrix}^{\pm 1}\} \subset \mathrm{GL}_2$$

• S_λ generates a group of affine transformations of $\mathbb{C}$, $x \mapsto \lambda x + 1$ and $x \mapsto \lambda x - 1$.
• it has polynomial growth iff λ is a root of unity.

Easy observation:

- if λ is not a root of a polynomial with coefficients in $\{-1, 0, 1\}$, then $\rho(S_\lambda) = 2$,
- if it is, then $\rho(S_\lambda) := \lim |S_\lambda^n|^{1/n} \leqslant M_\lambda$

where M_λ is the Mahler measure of λ.

Mahler measure and Lehmer conjecture

Let $\lambda \in \overline{\mathbb{Q}}^*$ be an algebraic number, and

$$\pi_\lambda := a_d X^d + \ldots + a_1 X + a_0$$

its minimal polynomial in $\mathbb{Z}[X]$. Factorize it as

$$\pi_\lambda(X) = a_d \prod_1^d (X - x_i)$$

The Mahler measure of π_λ is the quantity:

$$M_\lambda := |a_d| \prod \max\{1, |x_i|\}.$$

Mahler measure and Lehmer conjecture

The Mahler measure of π_λ is the quantity:

$$M_\lambda := |a_d| \prod \max\{1, |x_i|\}.$$

Lehmer's conjecture (1930s): $\exists \varepsilon > 0$ s.t. $\forall \lambda \in \overline{\mathbb{Q}}^*$,

- either $M_\lambda = 1$ and λ is a root of unity,
- or $M_\lambda > 1 + \varepsilon$.

Mahler measure and Lehmer conjecture

The Mahler measure of π_λ is the quantity:

$$M_\lambda := |a_d| \prod \max\{1, |x_i|\}.$$

Lehmer's conjecture (1930s): $\exists \varepsilon > 0$ s.t. $\forall \lambda \in \overline{\mathbb{Q}}^*$,

- either $M_\lambda = 1$ and λ is a root of unity,
- or $M_\lambda > 1 + \varepsilon$.

Mahler measure and Lehmer conjecture

Lehmer's conjecture (1930s): $\exists \varepsilon > 0$ s.t. $\forall \lambda \in \overline{\mathbb{Q}}^*$,

- either $M_\lambda = 1$ and λ is a root of unity,
- or $M_\lambda > 1 + \varepsilon$.

Mahler measure and Lehmer conjecture

Lehmer's conjecture (1930s): $\exists \varepsilon > 0$ s.t. $\forall \lambda \in \overline{\mathbb{Q}}^*$,

- either $M_\lambda = 1$ and λ is a root of unity,
- or $M_\lambda > 1 + \varepsilon$.

$\rightarrow$ the smallest known Mahler measure > 1 is that of the polynomial $X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$ and is approximately $1,17628...$

Mahler measure and Lehmer conjecture

Lehmer's conjecture (1930s): $\exists \varepsilon > 0$ s.t. $\forall \lambda \in \overline{\mathbb{Q}}^*$,

- either $M_\lambda = 1$ and λ is a root of unity,
- or $M_\lambda > 1 + \varepsilon$.

$\rightarrow$ the smallest known Mahler measure > 1 is that of the polynomial $X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$ and is approximately $1,17628...$

If λ is not an algebraic unit, or not Galois conjugate to λ^{-1}, then M_λ is bounded away from 1. Same if λ is totally real, or has *small* Galois group (Amoroso-David).

Mahler measure and Lehmer conjecture

Lehmer's conjecture (1930s): $\exists\varepsilon > 0$ s.t. $\forall\lambda \in \overline{\mathbb{Q}}^*$,

- either $M_\lambda = 1$ and λ is a root of unity,
- or $M_\lambda > 1 + \varepsilon$.

Suppose λ is an algebraic integer.

If all conjugates of λ except λ have modulus < 1, then λ is real > 1 and is called a Pisot number. Then $M_\lambda = \lambda$ and is known to be bounded away from 1 (Siegel).

Mahler measure and Lehmer conjecture

Lehmer's conjecture (1930s): $\exists \varepsilon > 0$ s.t. $\forall \lambda \in \overline{\mathbb{Q}}^*$,

- either $M_\lambda = 1$ and λ is a root of unity,
- or $M_\lambda > 1 + \varepsilon$.

Suppose λ is an algebraic integer.

If all conjugates of λ except λ have modulus < 1, then λ is real > 1 and is called a Pisot number. Then $M_\lambda = \lambda$ and is known to be bounded away from 1 (Siegel).

If all conjugates of λ except λ have modulus $\leqslant 1$, with at least one of modulus 1, then λ is real > 1 and is called a Salem number. Then $M_\lambda = \lambda$, but the conjecture is open for Salem numbers.

Back to the Uniform Growth Conjecture

Conjecture (Uniform growth conjecture)

Given $d \in \mathbb{N}$*, there is* $\varepsilon(d) > 0$ *such that for every finite symmetric* $S \subset \mathsf{GL}_d(\mathbb{C})$,

- *either* $\rho(S) = 1$
- *or* $\rho(S) > 1 + \varepsilon$.

Back to the Uniform Growth Conjecture

Conjecture (Uniform growth conjecture)

Given $d \in \mathbb{N}$, there is $\varepsilon(d) > 0$ such that for every finite symmetric $S \subset \mathrm{GL}_d(\mathbb{C})$,

- *either $\rho(S) = 1$*
- *or $\rho(S) > 1 + \varepsilon$.*

Recall that for $S = S_\lambda \subset \mathrm{GL}_2(\mathbb{C})$ we had $\rho(S_\lambda) \leqslant M_\lambda$.

Immediate consequence:

The Uniform Growth Conjecture implies the Lehmer Conjecture.

Semisimple Lehmer

Theorem (B. 2008)

If $S \subset \mathrm{GL}_d(\overline{\mathbb{Q}})$ is finite, one can define a "non-commutative Mahler measure" of S as

$$M_S := \prod_v (\lim_n ||S^n||_v^{\frac{1}{n}}),$$

and prove that $\exists \varepsilon = \varepsilon(d) > 0$ s.t.

$$M_S > 1 + \varepsilon,$$

provided $\langle S \rangle$ is not solvable (up to finite index).

Semisimple Lehmer

Theorem (B. 2008)

If $S \subset \mathrm{GL}_d(\overline{\mathbb{Q}})$ is finite, one can define a "non-commutative Mahler measure" of S as

$$M_S := \prod_v (\lim_n ||S^n||_v^{\frac{1}{n}}),$$

and prove that $\exists \varepsilon = \varepsilon(d) > 0$ s.t.

$$M_S > 1 + \varepsilon,$$

provided $\langle S \rangle$ is not solvable (up to finite index).

Corollary

The uniform growth conjecture is true assuming $\langle S \rangle$ is not solvable (up to finite index).

Semisimple Lehmer

Theorem (B. 2008)

If $S \subset \mathrm{GL}_d(\overline{\mathbb{Q}})$ is finite, one can define a "non-commutative Mahler measure" of S as

$$M_S := \prod_v (\lim_n ||S^n||_v^{\frac{1}{n}}),$$

and prove that $\exists \varepsilon = \varepsilon(d) > 0$ s.t.

$$M_S > 1 + \varepsilon,$$

provided $\langle S \rangle$ is not solvable (up to finite index).

Corollary

The uniform growth conjecture is true assuming $\langle S \rangle$ is not solvable (up to finite index).

$\longrightarrow$ so remains the solvable case...

Lower bound on the growth exponent

Recall

$$S_\lambda := \{1, \begin{pmatrix} \lambda & 1 \\ 0 & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} \lambda & -1 \\ 0 & 1 \end{pmatrix}^{\pm 1}\} \subset \mathrm{GL}_2$$

Theorem (B.+Varjú 2015)

For every $\lambda \in \overline{\mathbb{Q}}$,

$$(\min\{2, M_\lambda\})^{0.44} \leqslant \rho(S_\lambda) \leqslant \min\{2, M_\lambda\}.$$

Lower bound on the growth exponent

Recall

$$S_\lambda := \{1, \begin{pmatrix} \lambda & 1 \\ 0 & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} \lambda & -1 \\ 0 & 1 \end{pmatrix}^{\pm 1}\} \subset \mathrm{GL}_2$$

Theorem (B.+Varjú 2015)

For every $\lambda \in \overline{\mathbb{Q}}$,

$$(\min\{2, M_\lambda\})^{0.44} \leqslant \rho(S_\lambda) \leqslant \min\{2, M_\lambda\}.$$

Rk: $\rho(S_\lambda) < 2$ iff λ is a root of a polynomial with coefficients in $\{-1, 0, 1\}$.

Corollary

The uniform growth conjecture is equivalent to the Lehmer conjecture.

Lehmer and finite fields

Reducing mod p in the previous theorem, we can derive:

Corollary (B+V)

The Lehmer conjecture is equivalent to the following counting problem in finite fields:
There exists $\varepsilon > 0$ *and functions* $p(n) \in \mathbb{N}$ *and* $\omega(n) \in \mathbb{N}$ *s.t.* $\forall n \in \mathbb{N}$, *for every prime* $p > p(n)$ *and every* $x \in \mathbb{F}_p^*$,

$$order(x) > \omega(n) \Rightarrow |S_x^n| > (1+\varepsilon)^n.$$

Lehmer and finite fields

Reducing mod p in the previous theorem, we can derive:

Corollary (B+V)

The Lehmer conjecture is equivalent to the following counting problem in finite fields:
There exists $\varepsilon > 0$ and functions $p(n) \in \mathbb{N}$ and $\omega(n) \in \mathbb{N}$ s.t. $\forall n \in \mathbb{N}$, for every prime $p > p(n)$ and every $x \in \mathbb{F}_p^*$,

$$order(x) > \omega(n) \Rightarrow |S_x^n| > (1+\varepsilon)^n.$$

$\longrightarrow$ related pb: how fast can you obtain all of $\mathbb{F}_p$ starting from 1 and applying at each step either a translation by 1 or a multiplication by x ?

Random walk entropy and growth

Proof of the thm:

How to lower bound the growth rate $\rho(S_\lambda)$?

Random walk entropy and growth

Proof of the thm:

How to lower bound the growth rate $\rho(S_\lambda)$?

naive way: pick a Galois conjugate of modulus > 1, take a power λ^k with $|\lambda^k| > 2$, then the two transformations $x \mapsto \lambda^k x + 1$ and $x \mapsto \lambda^k x - 1$ generate a free semi-group $\longrightarrow$ get a lower bound of the growth.

Random walk entropy and growth

Proof of the thm:

How to lower bound the growth rate $\rho(S_\lambda)$?

naive way: pick a Galois conjugate of modulus > 1, take a power λ^k with $|\lambda^k| > 2$, then the two transformations $x \mapsto \lambda^k x + 1$ and $x \mapsto \lambda^k x - 1$ generate a free semi-group $\longrightarrow$ get a lower bound of the growth.

$\longrightarrow$ problem: k may need to be very large, and in fact $\exists \lambda_n \in \overline{\mathbb{Q}}$ s.t. $S^n_{\lambda_n}$ contains no pairs of generators of a free sub-semigroup...

Random walk entropy and growth

Proof of the thm:

How to lower bound the growth rate $\rho(S_\lambda)$?

naive way: pick a Galois conjugate of modulus > 1, take a power λ^k with $|\lambda^k| > 2$, then the two transformations $x \mapsto \lambda^k x + 1$ and $x \mapsto \lambda^k x - 1$ generate a free semi-group $\longrightarrow$ get a lower bound of the growth.

$\longrightarrow$ problem: k may need to be very large, and in fact $\exists \lambda_n \in \overline{\mathbb{Q}}$ s.t. $S_{\lambda_n}^n$ contains no pairs of generators of a free sub-semigroup...

$\longrightarrow$ idea: use entropy.

Random walk entropy and growth

Let $\xi_0, \xi_1, \ldots, \xi_n, \ldots$ be iid coin flips $\xi_0 = \pm 1$ with probability $\frac{1}{2}$.

Random walk entropy and growth

Let $\xi_0, \xi_1, \ldots, \xi_n, \ldots$ be iid coin flips $\xi_0 = \pm 1$ with probability $\frac{1}{2}$.

Given $\lambda \in \mathbb{C}$, form

$$X_\lambda^{(n)} := \xi_0 + \xi_1 \lambda + \ldots + \xi_{n-1} \lambda^{n-1}.$$

Random walk entropy and growth

Let $\xi_0, \xi_1, \ldots, \xi_n, \ldots$ be iid coin flips $\xi_0 = \pm 1$ with probability $\frac{1}{2}$.

Given $\lambda \in \mathbb{C}$, form

$$X_\lambda^{(n)} := \xi_0 + \xi_1 \lambda + \ldots + \xi_{n-1} \lambda^{n-1}.$$

The entropy $H(X_\lambda^{(n)})$ satisfies:

$$H(X_\lambda^{(n)}) \leqslant \log |\operatorname{Supp}(X_\lambda^{(n)})| = \log |S_\lambda^n|.$$

Random walk entropy and growth

Let $\xi_0, \xi_1, \dots, \xi_n, \dots$ be iid coin flips $\xi_0 = \pm 1$ with probability $\frac{1}{2}$.

Given $\lambda \in \mathbb{C}$, form

$$X_\lambda^{(n)} := \xi_0 + \xi_1 \lambda + \ldots + \xi_{n-1} \lambda^{n-1}.$$

The entropy $H(X_\lambda^{(n)})$ satisfies:

$$H(X_\lambda^{(n)}) \leqslant \log |\operatorname{Supp}(X_\lambda^{(n)})| = \log |S_\lambda^n|.$$

In particular we have:

$$h_\lambda := \lim_n \frac{H(X_\lambda^{(n)})}{n} \leqslant \rho(S_\lambda).$$

Random walk entropy and growth

In particular we have:

$$h_\lambda := \lim_n \frac{H(X_\lambda^{(n)})}{n} \leqslant \rho(S_\lambda).$$

We prove:

Theorem

For every $\lambda \in \overline{\mathbb{Q}} \setminus \{0\}$,

$$(\min\{1, \log_2 M_\lambda\})^{0.44} \leqslant h_\lambda \leqslant \min\{1, \log_2 M_\lambda\}.$$

Bernoulli convolutions

If λ has modulus < 1, then the series converges:

$$X^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

Bernoulli convolutions

If λ has modulus < 1, then the series converges:

$$X^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

The limit law is a Bernoulli convolution with parameter λ.

Bernoulli convolutions

If λ has modulus < 1, then the series converges:

$$X^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

The limit law is a Bernoulli convolution with parameter λ.
It is self-similar: $X^{(\infty)} = X^{(n)} + \lambda^n X'^{(\infty)}$.

Bernoulli convolutions

If λ has modulus < 1, then the series converges:

$$X^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

The limit law is a Bernoulli convolution with parameter λ.
It is self-similar: $X^{(\infty)} = X^{(n)} + \lambda^n X'^{(\infty)}$.

$$H(X^{(n)}) \quad \simeq \quad H(X^{(\infty)}; \lambda^n) \tag{1}$$

Bernoulli convolutions

If λ has modulus < 1, then the series converges:

$$X^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

The limit law is a Bernoulli convolution with parameter λ.
It is self-similar: $X^{(\infty)} = X^{(n)} + \lambda^n X'^{(\infty)}$.

$$H(X^{(n)}) \simeq H(X^{(\infty)}; \lambda^n) \quad (1)$$

$$\simeq \sum_{1}^{n} H(X^{(\infty)}; \lambda^i | \lambda^{i-1}) \quad (2)$$

Bernoulli convolutions

If λ has modulus < 1, then the series converges:

$$X^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

The limit law is a Bernoulli convolution with parameter λ.
It is self-similar: $X^{(\infty)} = X^{(n)} + \lambda^n X'^{(\infty)}$.

$$\begin{aligned}
H(X^{(n)}) &\simeq H(X^{(\infty)}; \lambda^n) && (1)\\
&\simeq \sum_1^n H(X^{(\infty)}; \lambda^i | \lambda^{i-1}) && (2)\\
&\simeq \sum_1^n H(X^{(i-1)} + \lambda^{i-1} X^{(\infty)}; \lambda^i | \lambda^{i-1}) && (3)
\end{aligned}$$

Bernoulli convolutions

If λ has modulus < 1, then the series converges:

$$X^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

The limit law is a Bernoulli convolution with parameter λ.
It is self-similar: $X^{(\infty)} = X^{(n)} + \lambda^n X'^{(\infty)}$.

$$\begin{aligned}
H(X^{(n)}) &\simeq H(X^{(\infty)}; \lambda^n) && (1)\\
&\simeq \sum_1^n H(X^{(\infty)}; \lambda^i | \lambda^{i-1}) && (2)\\
&\simeq \sum_1^n H(X^{(i-1)} + \lambda^{i-1} X^{(\infty)}; \lambda^i | \lambda^{i-1}) && (3)\\
&\geqslant \sum_1^n H(\lambda^{i-1} X^{(\infty)}; \lambda^i | \lambda^{i-1}) && (4)
\end{aligned}$$

Bernoulli convolutions

If λ has modulus < 1, then the series converges:

$$X^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

The limit law is a Bernoulli convolution with parameter λ.
It is self-similar: $X^{(\infty)} = X^{(n)} + \lambda^n X'^{(\infty)}$.

$$\begin{aligned}
H(X^{(n)}) &\simeq H(X^{(\infty)}; \lambda^n) && (1)\\
&\simeq \sum_1^n H(X^{(\infty)}; \lambda^i | \lambda^{i-1}) && (2)\\
&\simeq \sum_1^n H(X^{(i-1)} + \lambda^{i-1} X^{(\infty)}; \lambda^i | \lambda^{i-1}) && (3)\\
&\geqslant \sum_1^n H(\lambda^{i-1} X^{(\infty)}; \lambda^i | \lambda^{i-1}) && (4)\\
&\simeq nH(X^{(\infty)}; \lambda | 1) \geqslant nH(\xi_0; \lambda | 1) && (5)
\end{aligned}$$

Bernoulli convolutions

Taking the limit as $n \to \infty$ we get:

$$h_\lambda \gg |\log \lambda|.$$

Bernoulli convolutions

Taking the limit as $n \to \infty$ we get:

$$h_\lambda \gg |\log \lambda|.$$

good but not enough: we want the Mahler measure:

Bernoulli convolutions

Taking the limit as $n \to \infty$ we get:

$$h_\lambda \gg |\log \lambda|.$$

good but not enough: we want the Mahler measure:
$\longrightarrow$ idea: perform the above analysis in the geometric embedding of $\mathbb{Q}(\lambda)$ in $\mathbb{C}^d$, where d is the number of conjugates of modulus < 1.

Bernoulli convolutions

Taking the limit as $n \to \infty$ we get:

$$h_\lambda \gg |\log \lambda|.$$

good but not enough: we want the Mahler measure:
$\longrightarrow$ idea: perform the above analysis in the geometric embedding of $\mathbb{Q}(\lambda)$ in $\mathbb{C}^d$, where d is the number of conjugates of modulus < 1.

issues: (a) need an estimate independent of d ;

Bernoulli convolutions

Taking the limit as $n \to \infty$ we get:

$$h_\lambda \gg |\log \lambda|.$$

good but not enough: we want the Mahler measure:
$\longrightarrow$ idea: perform the above analysis in the geometric embedding of $\mathbb{Q}(\lambda)$ in $\mathbb{C}^d$, where d is the number of conjugates of modulus < 1.

issues: (a) need an estimate independent of d ; (b) no canonical way to discretize the space.

Bernoulli convolutions

Taking the limit as $n \to \infty$ we get:

$$h_\lambda \gg |\log \lambda|.$$

good but not enough: we want the Mahler measure:
$\longrightarrow$ idea: perform the above analysis in the geometric embedding of $\mathbb{Q}(\lambda)$ in $\mathbb{C}^d$, where d is the number of conjugates of modulus < 1.

issues: (a) need an estimate independent of d ; (b) no canonical way to discretize the space.

Nevertheless this can be done using *multivariate gaussians* in lieu of intervals as a means to discretize:

$$H(X; A) := H(X + AG) - H(AG)$$

for $A \in M_d(\mathbb{R})$ and $G =$ normalized in $\mathbb{R}^d$.

Bernoulli convolutions

Taking the limit as $n \to \infty$ we get:

$$h_\lambda \gg |\log \lambda|.$$

good but not enough: we want the Mahler measure:
$\longrightarrow$ idea: perform the above analysis in the geometric embedding of $\mathbb{Q}(\lambda)$ in $\mathbb{C}^d$, where d is the number of conjugates of modulus < 1.

issues: (a) need an estimate independent of d ; (b) no canonical way to discretize the space.

The subadditivity of this gaussian entropies is guaranteed by the submodularity property of the entropy:
If X, Y, Z are independent random variables in $\mathbb{R}^d$, then

$$H(X + Y + Z) + H(Y) \leqslant H(X + Y) + H(Y + Z).$$

Bernoulli convolutions for real parameter

Now take $\lambda \in (0, 1)$. Recall:

$$X_\lambda^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

Bernoulli convolutions for real parameter

Now take $\lambda \in (0,1)$. Recall:

$$X_\lambda^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

Erdös: how is the regularity of the law μ_λ of $X_\lambda^{(\infty)}$ depending on λ.

Bernoulli convolutions for real parameter

Now take $\lambda \in (0, 1)$. Recall:

$$X_\lambda^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

Erdös: how is the regularity of the law μ_λ of $X_\lambda^{(\infty)}$ depending on λ.

- μ_λ is either singular or absolutely continuous (self-similarity).

Bernoulli convolutions for real parameter

Now take $\lambda \in (0,1)$. Recall:

$$X_\lambda^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

Erdös: how is the regularity of the law μ_λ of $X_\lambda^{(\infty)}$ depending on λ.

- μ_λ is either singular or absolutely continuous (self-similarity).
- μ_λ is singular if $\lambda \in (0, \frac{1}{2})$ or if λ^{-1} is Pisot (only examples known in $(\frac{1}{2}, 1)$.)

Bernoulli convolutions for real parameter

Now take $\lambda \in (0,1)$. Recall:

$$X_\lambda^{(\infty)} = \sum_{i \geqslant 0} \xi_i \lambda^i,$$

Erdös: how is the regularity of the law μ_λ of $X_\lambda^{(\infty)}$ depending on λ.

- μ_λ is either singular or absolutely continuous (self-similarity).
- μ_λ is singular if $\lambda \in (0, \frac{1}{2})$ or if λ^{-1} is Pisot (only examples known in $(\frac{1}{2}, 1)$.)
- μ_λ is absolutely continuous for Lebesgue almost all λ near one (Erdös) and in fact on all $(\frac{1}{2}, 1)$ (Solomyak), and actually the singular λ have Hausdorff dimension zero (Hochman,Shmerkin 2014).

Bernoulli convolutions for real parameter $\lambda \in (\frac{1}{2}, 1)$

Hochman (2014) obtained a formula for the dimension of μ_λ. He showed that unless λ satisfies a strong diophantine condition, then

$$\dim \mu_\lambda = \min\{1, \frac{h_\lambda}{\log \lambda^{-1}}\}.$$

Bernoulli convolutions for real parameter $\lambda \in (\frac{1}{2}, 1)$

Hochman (2014) obtained a formula for the dimension of μ_λ. He showed that unless λ satisfies a strong diophantine condition, then

$$\dim \mu_\lambda = \min\{1, \frac{h_\lambda}{\log \lambda^{-1}}\}.$$

$E_n := \{$polynomials of degree $\leqslant n$ and coefficients in $-1, 0, 1\}$

Diophantine condition: $\forall n, \exists P_n \in E_n$ s.t. $P_n(\lambda) \to 0$ exponentially fast (but $\neq 0$).

Corollary (Hochman)

If the roots of all polynomials in E_n are exponentially separated, then $\dim \mu_\lambda = 1$ *for all* $\lambda \notin \overline{\mathbb{Q}}$.

Bernoulli convolutions for real parameter $\lambda \in (\frac{1}{2}, 1)$

Theorem (B+V 2016)

If $\dim \mu_\lambda < 1$, *then* λ *admits extremely good algebraic approximations, i.e. given* $A > 1$ *there are arbitrarily large* $d \in \mathbb{N}$ *such that*

$$\min_{\alpha \in E_d, \dim \mu_\alpha < 1} |\lambda - \alpha| < \exp(-d^A).$$

Bernoulli convolutions for real parameter $\lambda \in (\frac{1}{2}, 1)$

Theorem (B+V 2016)

If $\dim \mu_\lambda < 1$, *then* λ *admits extremely good algebraic approximations, i.e. given* $A > 1$ *there are arbitrarily large* $d \in \mathbb{N}$ *such that*

$$\min_{\alpha \in E_d, \dim \mu_\alpha < 1} |\lambda - \alpha| < \exp(-d^A).$$

Corollary

Many explicit transcendental numbers (e.g. $\lambda = \ln 2, e^{-\frac{1}{2}}, \frac{\pi}{4}$*) have* $\dim \mu_\lambda = 1$.

Bernoulli convolutions for real parameter $\lambda \in (\frac{1}{2}, 1)$

Theorem (B+V 2016)

If $\dim \mu_\lambda < 1$*, then* λ *admits extremely good algebraic approximations, i.e. given* $A > 1$ *there are arbitrarily large* $d \in \mathbb{N}$ *such that*

$$\min_{\alpha \in E_d, \dim \mu_\alpha < 1} |\lambda - \alpha| < \exp(-d^A).$$

Corollary

Many explicit transcendental numbers (e.g. $\lambda = \ln 2, e^{-\frac{1}{2}}, \frac{\pi}{4}$*) have* $\dim \mu_\lambda = 1$.

Corollary

The set of algebraic singular λ *is dense in the set of singular* λ.

Bernoulli convolutions for real parameter $\lambda \in (\frac{1}{2}, 1)$

Recall that Pisot numbers form a closed set (Salem 1940's).

Corollary

If the inverse Pisot numbers are the only algebraic singular λ, then they are the only singular λ.

Bernoulli convolutions for real parameter $\lambda \in (\frac{1}{2}, 1)$

Recall that Pisot numbers form a closed set (Salem 1940's).

Corollary

If the inverse Pisot numbers are the only algebraic singular λ, then they are the only singular λ.

Corollary

If Lehmer holds, then $\dim \mu_\lambda = 1$ *for all* λ *in an interval near* 1.

Bernoulli convolutions for real parameter $\lambda \in (\frac{1}{2}, 1)$

Recall that Pisot numbers form a closed set (Salem 1940's).

Corollary

If the inverse Pisot numbers are the only algebraic singular λ, then they are the only singular λ.

Corollary

If Lehmer holds, then $\dim \mu_\lambda = 1$ for all λ in an interval near 1.

$\longrightarrow$ reduces the dimension problem to algebraic numbers, where via Hochman's formula, the question is reduced to evaluating the discrete entropy h_λ.

Bernoulli convolutions for real parameter $\lambda \in (\frac{1}{2}, 1)$

Recall that Pisot numbers form a closed set (Salem 1940's).

Corollary

If the inverse Pisot numbers are the only algebraic singular λ, then they are the only singular λ.

Corollary

If Lehmer holds, then $\dim \mu_\lambda = 1$ *for all* λ *in an interval near* 1.

$\longrightarrow$ reduces the dimension problem to algebraic numbers, where via Hochman's formula, the question is reduced to evaluating the discrete entropy h_λ.

$\longrightarrow$ recent work by Péter Varjú goes further in the algebraic case getting μ_λ to be absolutely continuous for many algebraic λ.

The End!