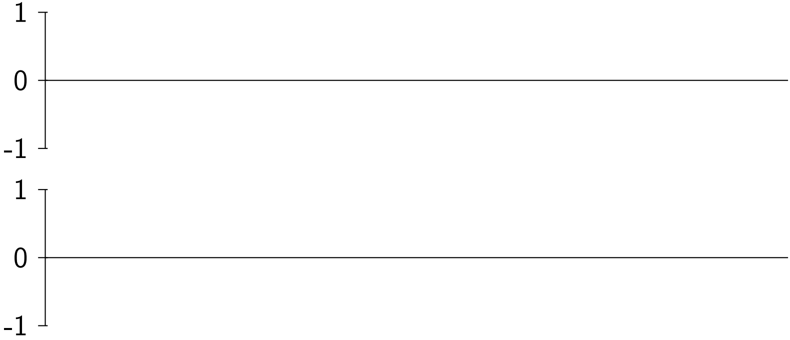
Entropy and independence in symbolic dynamics

Dominik Kwietniak
based on a joint work with
Marcin Kulczycki (UJ) and Jian Li (Shantou)

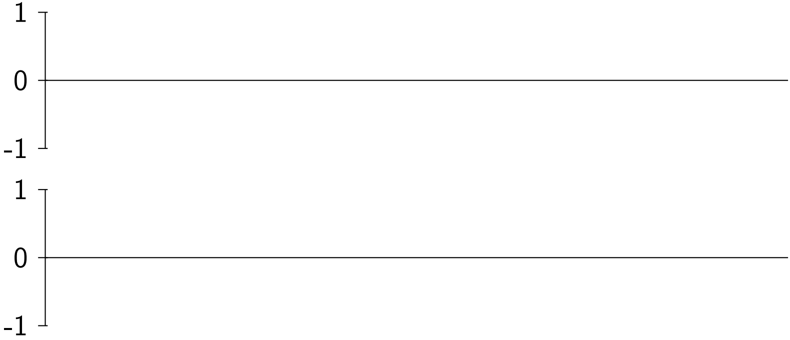
JAGIELLONIAN
UNIVERSITY
IN KRAKOW

Tossa de Mar, October 2, 2014

An Enigma

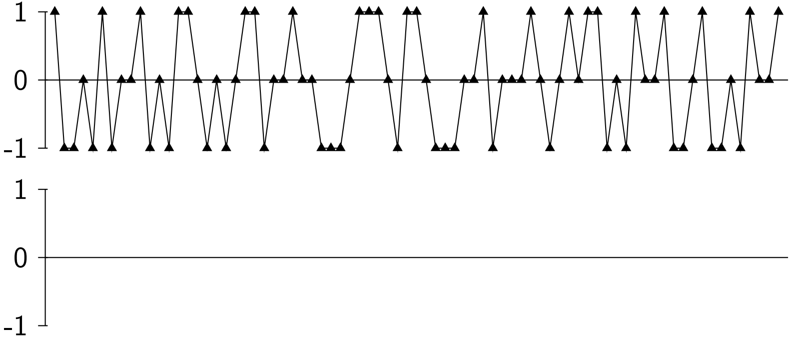


An Enigma



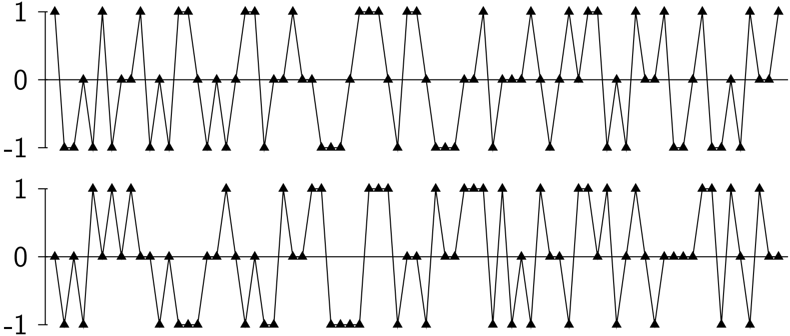
Which of these strings is generated at random?

An Enigma



Which of these strings is generated at random?

An Enigma



Which of these strings is generated at random?

The Möbius function

Let $n \in \mathbb{N} = \{1, 2, \ldots\}$. For $n \geq 2$ let $\langle n \rangle$ be the number of distinct prime factors of n.

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n \text{ is not square-free}, \\ (-1)^{\langle n \rangle}, & \text{if } n \text{ is square-free}. \end{cases}$$

Is the sequence $(\mu(n))_{n=1}^{\infty}$ random?

From sequences to dynamical systems

Given a sequence $x = (x_i)_{i=1}^{\infty} \in \{0,1\}^{\mathbb{N}}$ we consider the shift space X which is the closure of the orbit of x with respect to the shift map σ, that is

$$X = \overline{\{\sigma^n(x) : n \geq 0\}}.$$

From sequences to dynamical systems

Given a sequence $x = (x_i)_{i=1}^{\infty} \in \{0,1\}^{\mathbb{N}}$ we consider the shift space X which is the closure of the orbit of x with respect to the shift map σ, that is

$$X = \overline{\{\sigma^n(x) : n \geq 0\}}.$$

Definition

A square-free flow is a shift space generated as above by the sequence $\eta(n) = \mu^2(n)$.

Which sequences are random?

A heuristic is: a sequence is random if it is orthogonal to a deterministic one. Which sequences are deterministic? Those who come from a zero entropy homeomorphisms.

Shift spaces

Shift spaces

Definition

Let $\mathcal{A} = \{0, 1, \ldots, r - 1\}$ be an alphabet.

Shift spaces

Definition

Let $\mathcal{A} = \{0, 1, \ldots, r-1\}$ be an alphabet. The full r-shift is

$$\mathcal{A}^{\mathbb{N}} = \{x = (x_i)_{i=1}^{\infty} : x_i \in \mathcal{A} \text{ for all } i \in \mathbb{N}\}.$$

Shift spaces

Definition

Let $\mathcal{A} = \{0, 1, \ldots, r-1\}$ be an alphabet. The full r-shift is

$$\mathcal{A}^{\mathbb{N}} = \{x = (x_i)_{i=1}^{\infty} : x_i \in \mathcal{A} \text{ for all } i \in \mathbb{N}\}.$$

The shift map $\sigma \colon \mathcal{A}^{\mathbb{N}} \mapsto \mathcal{A}^{\mathbb{N}}$ maps $x = (x_i)_{i=1}^{\infty}$ to the sequence $\sigma(x) = (x_{i+1})_{i=1}^{\infty}$.

Shift spaces

Definition

Let $\mathcal{A} = \{0, 1, \ldots, r-1\}$ be an alphabet. The full r-shift is

$$\mathcal{A}^{\mathbb{N}} = \{x = (x_i)_{i=1}^{\infty} : x_i \in \mathcal{A} \text{ for all } i \in \mathbb{N}\}.$$

The shift map $\sigma \colon \mathcal{A}^{\mathbb{N}} \mapsto \mathcal{A}^{\mathbb{N}}$ maps $x = (x_i)_{i=1}^{\infty}$ to the sequence $\sigma(x) = (x_{i+1})_{i=1}^{\infty}$. A shift space is any closed σ-invariant subset of $\mathcal{A}^{\mathbb{N}}$.

The language of a shift space

The language of a shift space

Definition

A block over $\mathcal{A}$ is a finite sequence of symbols from $\mathcal{A}$. An n-block stands for a block of length n.

The language of a shift space

Definition

A block over $\mathcal{A}$ is a finite sequence of symbols from $\mathcal{A}$. An n-block stands for a block of length n.

The language of a shift space

Definition

A block over $\mathcal{A}$ is a finite sequence of symbols from $\mathcal{A}$. An n-block stands for a block of length n. The set of all blocks over $\mathcal{A}$ is denoted by $\mathcal{A}^*$.

The language of a shift space

Definition

A block over $\mathcal{A}$ is a finite sequence of symbols from $\mathcal{A}$. An n-block stands for a block of length n. The set of all blocks over $\mathcal{A}$ is denoted by $\mathcal{A}^*$. Let $x = (x_i)_{i=1}^{\infty} \in \mathcal{A}^{\mathbb{N}}$.

$$\dots x_{i-1} \underbrace{\boxed{x_i \; x_{i+1} \dots x_{j-1} \; x_j}}_{x_{[i,j]}} x_{j+1} \dots$$

The language of a shift space

Definition

A block over $\mathcal{A}$ is a finite sequence of symbols from $\mathcal{A}$. An n-block stands for a block of length n. The set of all blocks over $\mathcal{A}$ is denoted by $\mathcal{A}^*$. Let $x = (x_i)_{i=1}^{\infty} \in \mathcal{A}^{\mathbb{N}}$.

$$\dots x_{i-1} \underbrace{\boxed{x_i \ x_{i+1} \dots x_{j-1} \ x_j}}_{x_{[i,j]}} x_{j+1} \dots$$

A block $w \in A^*$ occurs in x if $w = x_{[i,j]}$ for some $1 \leq i \leq j < \infty$.

The language of a shift space

Definition

A block over $\mathcal{A}$ is a finite sequence of symbols from $\mathcal{A}$. An n-block stands for a block of length n. The set of all blocks over $\mathcal{A}$ is denoted by $\mathcal{A}^*$. Let $x = (x_i)_{i=1}^{\infty} \in \mathcal{A}^{\mathbb{N}}$.

$$\dots x_{i-1} \underbrace{\boxed{x_i \; x_{i+1} \dots x_{j-1} \; x_j}}_{x_{[i,j]}} x_{j+1} \dots$$

A block $w \in A^*$ occurs in x if $w = x_{[i,j]}$ for some $1 \leq i \leq j < \infty$.

Definition

A language of a shift space X is the set $Bl(X)$ of all blocks which do occur in some sequence $x \in X$.

The language of a shift space

Definition

A block over $\mathcal{A}$ is a finite sequence of symbols from $\mathcal{A}$. An n-block stands for a block of length n. The set of all blocks over $\mathcal{A}$ is denoted by $\mathcal{A}^*$. Let $x = (x_i)_{i=1}^{\infty} \in \mathcal{A}^{\mathbb{N}}$.

$$\dots x_{i-1} \underbrace{\boxed{x_i \; x_{i+1} \dots x_{j-1} \; x_j}}_{x_{[i,j]}} x_{j+1} \dots$$

A block $w \in A^*$ occurs in x if $w = x_{[i,j]}$ for some $1 \leq i \leq j < \infty$.

Definition

A language of a shift space X is the set $Bl(X)$ of all blocks which do occur in some sequence $x \in X$. We write $\mathcal{B}_n(X)$ for the set of all n-blocks contained in $\mathcal{B}(X)$.

Topological entropy

Topological entropy

Definition

The entropy of a shift space X is

$$h(X) = \lim_{n\to\infty} \frac{1}{n} \log |\mathcal{B}_n(X)| = \inf_{n\geq 1} \frac{1}{n} \log |\mathcal{B}_n(X)|.$$

Subordinate shift

Subordinate shift

Definition

A block $w = w_1 \dots w_k \in \mathcal{A}^*$ ($x \in \mathcal{A}^{\mathbb{N}}$) dominates a block $v = v_1 \dots v_k \in \mathcal{A}^*$ ($y \in \mathcal{A}^{\mathbb{N}}$) if $v_i \leq w_i$ for $i = 1, \dots, k$ ($y_i \leq x_i$ for $i \in \mathbb{N}$).

Subordinate shift

Definition

A block $w = w_1 \dots w_k \in \mathcal{A}^*$ ($x \in \mathcal{A}^{\mathbb{N}}$) dominates a block $v = v_1 \dots v_k \in \mathcal{A}^*$ ($y \in \mathcal{A}^{\mathbb{N}}$) if $v_i \leq w_i$ for $i = 1, \dots, k$ ($y_i \leq x_i$ for $i \in \mathbb{N}$).

Subordinate shift

Definition

A block $w = w_1 \dots w_k \in \mathcal{A}^*$ ($x \in \mathcal{A}^{\mathbb{N}}$) dominates a block $v = v_1 \dots v_k \in \mathcal{A}^*$ ($y \in \mathcal{A}^{\mathbb{N}}$) if $v_i \le w_i$ for $i = 1, \dots, k$ ($y_i \le x_i$ for $i \in \mathbb{N}$).

Definition

A subordinate of $\mathcal{L} \subset \mathcal{A}^*$ is the set $\mathcal{L}^{\le}$ of all $v \in \mathcal{A}^*$ that are dominated by some $w \in \mathcal{L}$.

Subordinate shift

Definition

A block $w = w_1 \ldots w_k \in \mathcal{A}^*$ ($x \in \mathcal{A}^{\mathbb{N}}$) dominates a block $v = v_1 \ldots v_k \in \mathcal{A}^*$ ($y \in \mathcal{A}^{\mathbb{N}}$) if $v_i \leq w_i$ for $i = 1, \ldots, k$ ($y_i \leq x_i$ for $i \in \mathbb{N}$).

Definition

A subordinate of $\mathcal{L} \subset \mathcal{A}^*$ is the set $\mathcal{L}^{\leq}$ of all $v \in \mathcal{A}^*$ that are dominated by some $w \in \mathcal{L}$.

Subordinate shift

Definition

A block $w = w_1 \dots w_k \in \mathcal{A}^*$ ($x \in \mathcal{A}^{\mathbb{N}}$) dominates a block $v = v_1 \dots v_k \in \mathcal{A}^*$ ($y \in \mathcal{A}^{\mathbb{N}}$) if $v_i \leq w_i$ for $i = 1, \dots, k$ ($y_i \leq x_i$ for $i \in \mathbb{N}$).

Definition

A subordinate of $\mathcal{L} \subset \mathcal{A}^*$ is the set $\mathcal{L}^{\leq}$ of all $v \in \mathcal{A}^*$ that are dominated by some $w \in \mathcal{L}$.

Definition

Given a point $x \in \mathcal{A}^{\mathbb{N}}$, a subordinate shift of x, denoted by $X^{\leq x}$, is a shift space given by the language $\mathcal{B}_x^{\leq}$, where $\mathcal{B}_x$ is the language of x.

Subordinate shift

Definition

A block $w = w_1 \dots w_k \in \mathcal{A}^*$ ($x \in \mathcal{A}^{\mathbb{N}}$) dominates a block $v = v_1 \dots v_k \in \mathcal{A}^*$ ($y \in \mathcal{A}^{\mathbb{N}}$) if $v_i \leq w_i$ for $i = 1, \dots, k$ ($y_i \leq x_i$ for $i \in \mathbb{N}$).

Definition

A subordinate of $\mathcal{L} \subset \mathcal{A}^*$ is the set $\mathcal{L}^{\leq}$ of all $v \in \mathcal{A}^*$ that are dominated by some $w \in \mathcal{L}$.

Definition

Given a point $x \in \mathcal{A}^{\mathbb{N}}$, a subordinate shift of x, denoted by $X^{\leq x}$, is a shift space given by the language $\mathcal{B}_x^{\leq}$, where $\mathcal{B}_x$ is the language of x.

(Remark: Subordinate shifts are *hereditary*.)

Examples

Examples

Lemma

Square-free flow is a subordinate shift.

Examples

Lemma

Square-free flow is a subordinate shift.

As a consequence the combinatorial patterns appearing in its characteristic function are chaotic...

Independence set for a shift space

Independence set for a shift space

Definition

We say that a set $J \subset \mathbb{N}$ is an independence set for a shift space $X \subset \mathcal{A}^{\mathbb{N}}$ if for every function $\varphi\colon J \to \mathcal{A}$ there is a point $x = \{x_j\}_{j=1}^{\infty} \in X$ such that $x_j = \varphi(j)$ for every $j \in J$.

Examples of independence sets

Examples of independence sets

Example

Any subset of $\mathbb{N}$ is an independence set for the full shift.

Examples of independence sets

Example

Any subset of $\mathbb{N}$ is an independence set for the full shift.

Example

A subset of $\mathbb{N}$ is an independence set for the golden mean shift if and only if it does not contain two consecutive integers.

Examples of independence sets

Example

Any subset of $\mathbb{N}$ is an independence set for the full shift.

Example

A subset of $\mathbb{N}$ is an independence set for the golden mean shift if and only if it does not contain two consecutive integers.

Example

If $J \subset \mathbb{N}$ is an independence set for a shift space X, then so is every subset of J.

Examples of independence sets

Example

Any subset of $\mathbb{N}$ is an independence set for the full shift.

Example

A subset of $\mathbb{N}$ is an independence set for the golden mean shift if and only if it does not contain two consecutive integers.

Example

If $J \subset \mathbb{N}$ is an independence set for a shift space X, then so is every subset of J.

Example

If X is a binary hereditary shift, then a $J \subset \mathbb{N}$ is an independence set for X if and only if its characteristic function belongs to X.

Densities

Densities

Definition

A set $A \subset \mathbb{N}$ has density α if the limit

$$d(A) = \lim_{n \to \infty} \frac{|A \cap \{1, 2, \ldots, n\}|}{n}$$

exists and is equal to α.

Densities

Definition

A set $A \subset \mathbb{N}$ has density α if the limit

$$d(A) = \lim_{n \to \infty} \frac{|A \cap \{1, 2, \dots, n\}|}{n}$$

exists and is equal to α.

Definition

The Shnirelman density of a set $A \subset \mathbb{N}$ is

$$d_{Sh}(A) = \inf_{n \geq 1} \left\{ \frac{|A \cap \{1, 2, \dots, n\}|}{n} : n \in \mathbb{N} \right\}.$$

Main theorem

Main theorem

Theorem

Let X be a binary shift. Then the entropy of X is positive if and only if X is independent over a set A whose density exists, is positive, and is equal to its Shnirelman density.

Limiting frequency

Limiting frequency

Definition

Let $a \in \mathcal{A}$ and $w = w_1 \ldots w_k \in \mathcal{A}^*$.

Limiting frequency

Definition

Let $a \in \mathcal{A}$ and $w = w_1 \dots w_k \in \mathcal{A}^*$. Define

$$||w||_a = |\{1 \leq j \leq k : w_j = a\}|,$$

Limiting frequency

Definition

Let $a \in \mathcal{A}$ and $w = w_1 \dots w_k \in \mathcal{A}^*$. Define

$$||w||_a = |\{1 \le j \le k : w_j = a\}|,$$
$$\mathsf{M}_k^a(X) = \max\{||w||_a : w \in \mathcal{B}_k(X)\}.$$

Limiting frequency

Definition

Let $a \in \mathcal{A}$ and $w = w_1 \dots w_k \in \mathcal{A}^*$. Define

$$||w||_a = |\{1 \leq j \leq k : w_j = a\}|,$$
$$\mathsf{M}_k^a(X) = \max\{||w||_a : w \in \mathcal{B}_k(X)\}.$$

The sequence $\{\mathsf{M}_k^a(X)\}_{k=1}^{\infty}$ is subadditive, that is

$$0 \leq \mathsf{M}_{m+n}^a(X) \leq \mathsf{M}_m^a(X) + \mathsf{M}_n^a(X) \quad n, m \in \mathbb{N}.$$

Limiting frequency

Definition

Let $a \in \mathcal{A}$ and $w = w_1 \dots w_k \in \mathcal{A}^*$. Define

$$||w||_a = |\{1 \leq j \leq k : w_j = a\}|,$$
$$\mathrm{M}_k^a(X) = \max\{||w||_a \,:\, w \in \mathcal{B}_k(X)\}.$$

The sequence $\{\mathrm{M}_k^a(X)\}_{k=1}^{\infty}$ is subadditive, that is

$$0 \leq \mathrm{M}_{m+n}^a(X) \leq \mathrm{M}_m^a(X) + \mathrm{M}_n^a(X) \quad n, m \in \mathbb{N}.$$

We define the limiting frequency of a in X by

$$\mathrm{Fr}_a(X) = \lim_{k\to\infty} \frac{\mathrm{M}_k^a(X)}{k} = \inf_{k\geq 1} \frac{\mathrm{M}_k^a(X)}{k}.$$

A topological consequence of maximal ergodic theorem

A topological consequence of maximal ergodic theorem

Definition

For $a \in \mathcal{A}$ and $x \in X$ define the characteristic set $\chi_a(x)$ as the set of positions at which a appears in x, that is,

$$\chi_a(x) = \{j \in \mathbb{N} : x_j = a\}.$$

A topological consequence of maximal ergodic theorem

Definition

For $a \in \mathcal{A}$ and $x \in X$ define the characteristic set $\chi_a(x)$ as the set of positions at which a appears in x, that is,

$$\chi_a(x) = \{j \in \mathbb{N} : x_j = a\}.$$

Theorem

Let X be a shift space over an alphabet $\mathcal{A}$. Then for every symbol $a \in \mathcal{A}$ there exists a point $\omega_a \in X$ such that

$$d_{Sh}(\chi_a(\omega_a)) = d(\chi_a(\omega_a)) = \mathrm{Fr}_a(X).$$

Independence sets for blocks

Independence sets for blocks

Definition

Let $\mathcal{F}$ be a (possibly empty) family of binary blocks of length $n \geq 0$.

Independence sets for blocks

Definition

Let $\mathcal{F}$ be a (possibly empty) family of binary blocks of length $n \geq 0$. We say that $\mathcal{F}$ is independent over a set $J \subset \mathbb{N}$ and J is an independence set for $\mathcal{F}$ if for each map $\varphi\colon J \to \{0, 1\}$ there is a block $w \in \mathcal{F}$ whose i-th symbol is $\varphi(i)$ for every $i \in J$.

Independence sets for blocks

Definition

Let $\mathcal{F}$ be a (possibly empty) family of binary blocks of length $n \geq 0$. We say that $\mathcal{F}$ is independent over a set $J \subset \mathbb{N}$ and J is an independence set for $\mathcal{F}$ if for each map $\varphi\colon J \to \{0, 1\}$ there is a block $w \in \mathcal{F}$ whose i-th symbol is $\varphi(i)$ for every $i \in J$.

Independence sets for blocks

Definition

Let $\mathcal{F}$ be a (possibly empty) family of binary blocks of length $n \geq 0$. We say that $\mathcal{F}$ is independent over a set $J \subset \mathbb{N}$ and J is an independence set for $\mathcal{F}$ if for each map $\varphi\colon J \to \{0, 1\}$ there is a block $w \in \mathcal{F}$ whose i-th symbol is $\varphi(i)$ for every $i \in J$. We denote the collection of all sets of independence for $\mathcal{F}$ by $\mathcal{I}(\mathcal{F})$.

Independence sets for blocks

Definition

Let $\mathcal{F}$ be a (possibly empty) family of binary blocks of length $n \geq 0$. We say that $\mathcal{F}$ is independent over a set $J \subset \mathbb{N}$ and J is an independence set for $\mathcal{F}$ if for each map $\varphi \colon J \to \{0, 1\}$ there is a block $w \in \mathcal{F}$ whose i-th symbol is $\varphi(i)$ for every $i \in J$. We denote the collection of all sets of independence for $\mathcal{F}$ by $\mathcal{I}(\mathcal{F})$. We assume the convention that the empty set is a set of independence for every (including empty) family of n-blocks.

Sauer-Perles^2-Shelah Lemma

Sauer-Perles^2-Shelah Lemma

Lemma (Sauer-Perles^2-Shelah)

Let $\mathcal{F} \subset \{0,1\}^n$ be a family of binary blocks of length $n \geq 1$. If for some $1 \leq k \leq n$ we have

$$|\mathcal{F}| > \sum_{j=0}^{k-1} \binom{n}{j},$$

then $\mathcal{F}$ is independent over some set of cardinality k.

Sauer-Perles^2-Shelah Lemma

Lemma (Sauer-Perles^2-Shelah)

Let $\mathcal{F} \subset \{0,1\}^n$ be a family of binary blocks of length $n \geq 1$. If for some $1 \leq k \leq n$ we have

$$|\mathcal{F}| > \sum_{j=0}^{k-1} \binom{n}{j},$$

then $\mathcal{F}$ is independent over some set of cardinality k.

Lemma (Pajor)

Let $\mathcal{F}$ be a family of binary blocks of length $n \geq 0$. Then $|\mathcal{I}(\mathcal{F})| \geq |\mathcal{F}|$.

Karpovsky-Milman

Lemma (Calculus)

Let $0 < \varepsilon \leq 1/2$ *and* $n \geq 1$. *Then*

$$\sum_{j=0}^{\lfloor n\varepsilon \rfloor} \binom{n}{j} \leq 2^{n \cdot H(\varepsilon)},$$

where $H(\varepsilon) = -\varepsilon \log \varepsilon - (1-\varepsilon)\log(1-\varepsilon)$.

Karpovsky-Milman

Lemma (Karpovsky-Milman)

Let X be a binary shift with positive topological entropy. Then there is an $\varepsilon > 0$ such that for every $n \geq 1$ there is a set $J \subset \{1, \ldots, n\}$ with $\lfloor \varepsilon n \rfloor$ elements which is an independence set for X.

Lemma (Calculus)

Let $0 < \varepsilon \leq 1/2$ and $n \geq 1$. Then

$$\sum_{j=0}^{\lfloor n\varepsilon \rfloor} \binom{n}{j} \leq 2^{n \cdot H(\varepsilon)},$$

where $H(\varepsilon) = -\varepsilon \log \varepsilon - (1-\varepsilon) \log(1-\varepsilon)$.

Entropy of subordinate shifts

Theorem

If $X^{\leq x}$ is a subordinate shift of x, then

$$\mathrm{Fr}_1(x) \leq h(X^{\leq x}) \leq \mathrm{Fr}_1(x) + h(x).$$

In particular, if $h(x) = 0$, then $h(X^{\leq x}) = \mathrm{Fr}_1(x)$.

Theorem

For every $t \in [0,1]$ there is a binary subordinate shift with entropy t.

Intrinsic ergodicity of subordinate shifts

Let $\mathcal{M}^{\mathsf{max}}(X)$ be the set of all measures of maximal entropy for X.

Theorem

If $X^{\leq x}$ is a subordinate shift of x and $h(x) = 0$ then $\mathcal{M}^{\mathsf{max}}(X) = \{\mu : \mu[1] = \mathsf{Fr}_1(x)\}$. In particular, if x is uniquely ergodic, then $X^{\leq x}$ is intrinsically ergodic.

Theorem

There is a mixing binary subordinate shift with uncountably many measures of maximal entropy.