Normality in non-integer bases and polynomial time randomness

Javier Almarza and Santiago Figueira

University of Buenos Aires

CMO BIRS 2016
Algorithmic Randomness Interacts with
Analysis and Ergodic Theory

Normality

- a weak notion of randomness
- introduced by Borel in 1909
- "law of large numbers" for blocks of events

Definition

Let $b \in \mathbb{N}, b \geq 2$, and $\Sigma = \{0, \ldots, b-1\}$.
A real x is **normal in base *b*** if for every string $\sigma \in \Sigma^*$

$$\lim_n \frac{\text{number of occurrences of } \sigma \text{ in the first } n \text{ digits of the expansion of } x \text{ in base } b}{n} = b^{-|\sigma|}$$

- almost all numbers are normal to all bases
- normality is not base invariant

Martingales

Definition

Let $b \in \mathbb{N}, b \geq 2$, and $\Sigma = \{0, \ldots, b-1\}$.
A **martingale in base b** is a function $f : \Sigma^* \to \mathbb{R}^{\geq 0}$ such that

$$f(\sigma) = b^{-1} \sum_{a \in \Sigma} f(\sigma a).$$

We say that M **succeeds** on $s \in \Sigma^{\mathbb{N}}$ iff

$$\limsup_n f(s \upharpoonright n) = \infty.$$

- A martingale is a formalization of a betting strategy
- $f(\sigma)$ is the capital of the gambler after having seen σ. He starts with an initial capital of $f(\emptyset)$
- The betting is *fair* in that the expected capital after the next bet is equal to the current capital

Outline

1. Normality for non-uniform measures and DFA martingales

Outline

1. Normality for non-uniform measures and DFA martingales

2. Normality for non-integer bases and polytime martingales

Outline

1. Normality for non-uniform measures and DFA martingales

2. Normality for non-integer bases and polytime martingales

Normality and martingales generated by finite automata

Definition (Schnorr & Stimm, 1972)

A martingale f is **generated by a DFA** if there is a DFA $M = \langle Q, \Sigma, \delta, q_0, Q_f \rangle$, and a function $g\colon Q \times \Sigma \to \mathbb{R}$ such that

$$f(\sigma a) = g(\delta^*(\sigma, q_0), a) f(\sigma)$$

for any word $\sigma \in \Sigma^*$ and symbol a.

- the betting factors $\frac{f(\sigma a)}{f(\sigma)}$ only depend on the instantaneous state $\delta^*(\sigma, q_0)$ and the symbol a
- the value of the betting factor is not *computed* by the DFA, just *selected* through g

Normality and martingales generated by finite automata

Definition (Schnorr & Stimm, 1972)

A martingale f is **generated by a DFA** if there is a DFA $M = \langle Q, \Sigma, \delta, q_0, Q_f \rangle$, and a function $g\colon Q \times \Sigma \to \mathbb{R}$ such that

$$f(\sigma a) = g(\delta^*(\sigma, q_0), a) f(\sigma)$$

for any word $\sigma \in \Sigma^*$ and symbol a.

- the betting factors $\frac{f(\sigma a)}{f(\sigma)}$ only depend on the instantaneous state $\delta^*(\sigma, q_0)$ and the symbol a
- the value of the betting factor is not *computed* by the DFA, just *selected* through g

Theorem (Schnorr & Stimm, 1972)

x is normal in base b if and only if no martingale in base b generated by a DFA succeeds on the expansion of x in base b.

We extend this result to “normality” for other measures, and “martingales” for other measures.

Subshifts

Let Σ be a finite alphabet.

Definition

A **subshift** is a tuple (X, T) where

- X is some closed subset of $\Sigma^{\mathbb{N}}$ with the product topology
- X is invariant under T, i.e. $T(X) \subseteq X$
- T is the continuous mapping defined by $(T(s))_n = s_{n+1}$.

Subshifts

Let Σ be a finite alphabet.

Definition

A **subshift** is a tuple (X, T) where

- X is some closed subset of $\Sigma^{\mathbb{N}}$ with the product topology
- X is invariant under T, i.e. $T(X) \subseteq X$
- T is the continuous mapping defined by $(T(s))_n = s_{n+1}$.

(X, T) is a subshift if and only if there exists a set $A \subseteq \Sigma^*$ such that X coincides with the set of sequences having no substrings in A.

- if A is finite then (X, T) is called a **Markov subshift** (or **subshift of finite type, SFT**)
- if A is a regular language then (X, T) is called **sofic subshift**

Examples of subshifts

The Cantor space $\{0,1\}^{\mathbb{N}}$ is the **full** subshift

Examples of subshifts

The Cantor space $\{0,1\}^{\mathbb{N}}$ is the **full** subshift

$$X = \text{sequences in } \{0,1\}^{\mathbb{N}} \text{ such that the next symbol after a 1 is always a 0}$$

is Markov: $A = \{11\}$

Examples of subshifts

The Cantor space $\{0,1\}^{\mathbb{N}}$ is the **full** subshift

$$X = \begin{array}{l}\text{sequences in } \{0,1\}^{\mathbb{N}} \text{ such that the next} \\ \text{symbol after a 1 is always a 0}\end{array}$$

is Markov: $A = \{11\}$

$$X = \text{ sequences in } \{0,1\}^{\mathbb{N}} \text{ with at most one occurrence of } 1$$

is not Markov but it is sofic: $A = 10^*1 = \{11, 101, 1001, 10001, \dots\}$

Normality for other measures

An **invariant** measure on a subshift (X, T) is a probability measure P on X such that $P \circ T^{-1} = P$.

Definition

Let P be an invariant measure. We say $s \in X$ is **distributed according to $\boldsymbol{P}$** if for all continuous $f\colon X \to \mathbb{R}$ we have

$$\lim_{N\to\infty} \frac{\sum_{n<N} f(T^n s)}{N} = \int f \; dP.$$

Normality for other measures

An **invariant** measure on a subshift (X, T) is a probability measure P on X such that $P \circ T^{-1} = P$.

Definition

Let P be an invariant measure. We say $s \in X$ is **distributed according to $\boldsymbol{P}$** if for all continuous $f\colon X \to \mathbb{R}$ we have

$$\lim_{N\to\infty} \frac{\sum_{n<N} f(T^n s)}{N} = \int f \, dP.$$

If X is the full subshift on $\Sigma = \{0, \ldots, b-1\}$ and $\lambda(a) = b^{-1}$ for $a \in \Sigma$ is the uniform measure then

s is distributed according to λ iff the real $0.s$ (written in base b) is normal in base b

Martingales for other measures

Definition

Let $L \subseteq \Sigma^*$ and let P be a probability measure P on $\Sigma^{\mathbb{N}}$ which is L-supported ($P(\sigma) > 0$ iff $\sigma \in L$).
A ***P*-martingale** is a function $f \colon L \to \mathbb{R}^{\geq 0}$ such that

$$f(\sigma) = \sum_{\substack{a \in \Sigma \\ \sigma a \in L}} P(\sigma a \mid \sigma) f(\sigma a).$$

Martingales for other measures

Definition

Let $L \subseteq \Sigma^*$ and let P be a probability measure P on $\Sigma^{\mathbb{N}}$ which is L-supported ($P(\sigma) > 0$ iff $\sigma \in L$).
A ***P*-martingale** is a function $f\colon L \to \mathbb{R}^{\geq 0}$ such that

$$f(\sigma) = \sum_{\substack{a \in \Sigma \\ \sigma a \in L}} P(\sigma a \mid \sigma) f(\sigma a).$$

When $P = \lambda$, the uniform measure on $\{0, \ldots, b-1\}$, the classical definition of a martingale is recovered:

$$\lambda(\sigma a \mid \sigma) = \lambda(a) = b^{-1}$$

The result by Schnorr & Stimm for Markov measures

Let L_X be the set of all words appearing in the sequences of X.

Theorem

Let (X, T) be a Markov subshift and let P be a L_X-supported Markov measure which is invariant and irreducible. Then $s \in X$ is distributed according to P iff no P-martingale generated by a DFA succeeds on s.

- the original Schnorr and Stimm's result is the special case when $X = \Sigma^{\mathbb{N}}$ and $P = \lambda$ is the uniform measure
- the Markov condition is used because we need some form of memorylessness on the measure to make it compatible with the memoryless computation of a finite automaton

Outline

1. Normality for non-uniform measures and DFA martingales
2. Normality for non-integer bases and polytime martingales

From integer to real bases

Proposition

Let $b \in \mathbb{N}, b > 1$.
x is normal in base b iff $(xb^n)_{n\in\mathbb{N}}$ is u.d. modulo one.

From integer to real bases

Proposition

Let $b \in \mathbb{N}, b > 1$.
x is normal in base b iff $(xb^n)_{n\in\mathbb{N}}$ is u.d. modulo one.

We propose to study this notion:

Definition (Normality for real bases)

Let $\beta \in \mathbb{R}$, $\beta > 1$.
x is **normal in base $\boldsymbol{\beta}$** iff $(x\beta^n)_{n\in\mathbb{N}}$ is u.d. modulo one.

By a result of Brown, Moran and Pearce (1986), there are irrational β's such that there are uncountably many reals x which are normal in any integer base but not normal in base β.

Normality and polytime computable martingales

Definition

x is **polynomial time random in base** $\boldsymbol{b}$ if no polynomial time computable martingale succeeds on the expansion of x in base b.

Normality and polytime computable martingales

Definition

x is **polynomial time random in base b** if no polynomial time computable martingale succeeds on the expansion of x in base b.

- polynomial time random in base $b \Rightarrow$ normal in base b (Schnorr 1971)
- polynomial time randomness is base invariant (F, Nies 2015)
  - polynomial time random in a single integer base $\geq 2 \Rightarrow$ normal for all integer bases ≥ 2

Question

polynomial time randomness $\Rightarrow$ normal in base $\beta \in \mathbb{Q}$ $(\beta > 1)$?

The formulation of normality in terms of u.d.

x is **normal in base $\boldsymbol{\beta}$** iff $(x\beta^n)_{n\in\mathbb{N}}$ is u.d. modulo one

If β is integer:

- the map
$$T_\beta(x) = (\beta x) \mod 1$$
is equivalent to a "shift" rightwards in the space of sequences $\{0,\ldots,\beta-1\}^{\mathbb{N}}$ when x is mapped to its expansion in base β

- $(x\beta^n) \mod 1 = T_\beta^n(x)$

The formulation of normality in terms of u.d.

x is **normal in base $\boldsymbol{\beta}$** iff $(x\beta^n)_{n\in\mathbb{N}}$ is u.d. modulo one

If β is integer:

- the map
$$T_\beta(x) = (\beta x) \mod 1$$
is equivalent to a "shift" rightwards in the space of sequences $\{0,\ldots,\beta-1\}^{\mathbb{N}}$ when x is mapped to its expansion in base β
    - if β is not integer, how to represent numbers in base β?
- $(x\beta^n) \mod 1 = T_\beta^n(x)$

The formulation of normality in terms of u.d.

x is **normal in base $\boldsymbol{\beta}$** iff $(x\beta^n)_{n\in\mathbb{N}}$ is u.d. modulo one

If β is integer:

- the map
$$T_\beta(x) = (\beta x) \mod 1$$
is equivalent to a "shift" rightwards in the space of sequences $\{0, \ldots, \beta - 1\}^{\mathbb{N}}$ when x is mapped to its expansion in base β
    - if β is not integer, how to represent numbers in base β?
- $(x\beta^n) \mod 1 = T_\beta^n(x)$
    - if β is not integer, this is false

β-expansions

Let $\beta \in \mathbb{R}$, $\beta > 1$. A **β-expansion** of x is

$$a_0 \,.\, a_1 \; a_2 \; a_3 \ldots$$

- $x = a_0 + \sum_{n>0} \frac{a_n}{\beta^n}$,
- $a_n \in \mathbb{N}$, and
- $0 \leq a_n < \beta$ for $n > 0$

β-expansions

Let $\beta \in \mathbb{R}$, $\beta > 1$. A **β-expansion** of x is

$$a_0 \;.\; a_1 \; a_2 \; a_3 \ldots$$

- $x = a_0 + \sum_{n>0} \frac{a_n}{\beta^n}$,
- $a_n \in \mathbb{N}$, and
- $0 \leq a_n < \beta$ for $n > 0$
- for all $n > 0$, $\sum_{i>n} a_i/\beta^i < 1/\beta^n$

β-expansions

Let $\beta \in \mathbb{R}$, $\beta > 1$. A **β-expansion** of x is

$$a_0 \;.\; a_1 \; a_2 \; a_3 \ldots$$

- $x = a_0 + \sum_{n>0} \frac{a_n}{\beta^n}$,
- $a_n \in \mathbb{N}$, and
- $0 \leq a_n < \beta$ for $n > 0$
- for all $n > 0$, $\sum_{i>n} a_i/\beta^i < 1/\beta^n$

Example

- $\beta = 2$:
  - The β-expansion of $3/4$ is $0.11000000000\ldots$

β-expansions

Let $\beta \in \mathbb{R}$, $\beta > 1$. A ***β*-expansion** of x is

$$a_0 \,.\, a_1 \; a_2 \; a_3 \ldots$$

- $x = a_0 + \sum_{n>0} \frac{a_n}{\beta^n}$,
- $a_n \in \mathbb{N}$, and
- $0 \leq a_n < \beta$ for $n > 0$
- for all $n > 0$, $\sum_{i>n} a_i/\beta^i < 1/\beta^n$

Example

- $\beta = 2$:
  - The β-expansion of $3/4$ is $0.11000000000\ldots$
  - The β-expansion of $2 \cdot 3/4$ is $1.10000000000\ldots$

β-expansions

Let $\beta \in \mathbb{R}$, $\beta > 1$. A **β-expansion** of x is

$$a_0 \ . \ a_1 \ a_2 \ a_3 \ldots$$

- $x = a_0 + \sum_{n>0} \frac{a_n}{\beta^n}$,
- $a_n \in \mathbb{N}$, and
- $0 \leq a_n < \beta$ for $n > 0$
- for all $n > 0$, $\sum_{i>n} a_i/\beta^i < 1/\beta^n$

Example

- $\beta = 2$:
  - The β-expansion of $3/4$ is $0.11000000000\ldots$
  - The β-expansion of $2 \cdot 3/4$ is $1.10000000000\ldots$
- $\beta = \phi$, the golden ratio ($\beta \approx 1.618$, $\beta^2 - \beta - 1 = 0$):
  - The β-expansion of $1/\beta$ is $0.1000000000\ldots$

β-expansions

Let $\beta \in \mathbb{R}$, $\beta > 1$. A ***β*-expansion** of x is

$$a_0 \,.\, a_1\ a_2\ a_3 \ldots$$

- $x = a_0 + \sum_{n>0} \frac{a_n}{\beta^n}$,
- $a_n \in \mathbb{N}$, and
- $0 \leq a_n < \beta$ for $n > 0$
- for all $n > 0$, $\sum_{i>n} a_i/\beta^i < 1/\beta^n$

Example

- $\beta = 2$:
  - The β-expansion of $3/4$ is $0.11000000000\ldots$
  - The β-expansion of $2 \cdot 3/4$ is $1.10000000000\ldots$
- $\beta = \phi$, the golden ratio ($\beta \approx 1.618$, $\beta^2 - \beta - 1 = 0$):
  - The β-expansion of $1/\beta$ is $0.1000000000\ldots$
  - The β-expansion of β is $1.10000000000\ldots$

β-expansions of 1

We are interested in the β-expansion of numbers in $[0, 1)$. We represent them simply by

$$\cancel{a_0}\,.\,a_1\ a_2\ a_3 \ldots$$

For the special case of 1, we extend the above representation by continuity (we force a_0 to be 0; the condition in red is not satisfied)

Example

- The 2-expansion of 1 is $11111111\ldots$ $(1 = \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \ldots)$
- The ϕ-expansion of 1 is $10101010\ldots$ $(1 = \frac{1}{\phi} + \frac{1}{\phi^3} + \frac{1}{\phi^5} + \frac{1}{\phi^7} + \ldots)$

β-shifts

Let $\Sigma = \{0, \ldots, \lceil\beta\rceil - 1]\}$. The β-expansions of $[0, 1)$ is the set

$$\{s \in \Sigma^{\mathbb{N}} \mid (\forall n)\ T^n s <_{\text{lex}} \text{the } \beta\text{-expansion of } 1\}$$

β-shifts

Let $\Sigma = \{0, \ldots, \lceil \beta \rceil - 1]\}$. The β-expansions of $[0, 1)$ is the set

$$\{s \in \Sigma^{\mathbb{N}} \mid (\forall n)\ T^n s <_{\text{lex}} \text{the } \beta\text{-expansion of } 1\}$$

Definition

The $\boldsymbol{\beta}$**-shift** is the subshift (X_β, T), where

$$X_\beta = \{s \in \Sigma^{\mathbb{N}} \mid (\forall n)\ T^n s \leq_{\text{lex}} \text{the } \beta\text{-expansion of } 1\}$$

β-shifts

Let $\Sigma = \{0, \ldots, \lceil \beta \rceil - 1]\}$. The β-expansions of $[0, 1)$ is the set

$$\{s \in \Sigma^{\mathbb{N}} \mid (\forall n)\ T^n s <_{\text{lex}} \text{the } \beta\text{-expansion of } 1\}$$

Definition

The **β-shift** is the subshift (X_β, T), where

$$X_\beta = \{s \in \Sigma^{\mathbb{N}} \mid (\forall n)\ T^n s \leq_{\text{lex}} \text{the } \beta\text{-expansion of } 1\}$$

Example

- The 2-shift is the full shift $\{0, 1\}^{\mathbb{N}}$
- The ϕ-shift is the set of sequences on $\{0, 1\}^{\mathbb{N}}$ such that no two 1's occur consecutively in them

Pisot numbers

Definition

$\beta \in \mathbb{R}$ is **Pisot** if $\beta > 1$ and β is the root of a monic polynomial in integer coefficients, such that all its conjugate values (that is, all the other roots of its minimal polynomial) have absolute values < 1.

Pisot numbers

Definition

$\beta \in \mathbb{R}$ is **Pisot** if $\beta > 1$ and β is the root of a monic polynomial in integer coefficients, such that all its conjugate values (that is, all the other roots of its minimal polynomial) have absolute values < 1.

Example

- all integers $n > 1$ are Pisot numbers
- rational Pisot numbers are integers
- the golden ratio $1.618\ldots$

Pisot numbers

Definition

$\beta \in \mathbb{R}$ is **Pisot** if $\beta > 1$ and β is the root of a monic polynomial in integer coefficients, such that all its conjugate values (that is, all the other roots of its minimal polynomial) have absolute values < 1.

Example

- all integers $n > 1$ are Pisot numbers
- rational Pisot numbers are integers
- the golden ratio $1.618\ldots$

Pisot numbers are "asymptotically integers" (Bertrand 1986):

β is Pisot iff $\sum_{n\geq 0}$ (distance from β^n to its closest integer) $< \infty$

Pisot numbers

Definition

$\beta \in \mathbb{R}$ is **Pisot** if $\beta > 1$ and β is the root of a monic polynomial in integer coefficients, such that all its conjugate values (that is, all the other roots of its minimal polynomial) have absolute values < 1.

Example

- all integers $n > 1$ are Pisot numbers
- rational Pisot numbers are integers
- the golden ratio $1.618\ldots$

Pisot numbers are "asymptotically integers" (Bertrand 1986):

$$\beta \text{ is Pisot} \quad \text{iff} \quad \sum_{n\geq 0} (\text{distance from } \beta^n \text{ to its closest integer}) < \infty$$

For β Pisot we have (Bertrand 1986):

- the β-expansion of 1 is eventually periodic and X_β is a sofic subshift
- if a real number x has a β-expansion that is distributed according to P_β (the Parry measure), then x is normal in base β

Putting all pieces together

Theorem

If x is polynomial time random then x is normal in base β for all Pisot β.

Putting all pieces together

Theorem

If x is polynomial time random then x is normal in base β for all Pisot β.

Proof sketch

- Suppose $(x\beta^n)_{n\in\mathbb{N}}$ is not u.d. mod 1. Let $s = \beta$-expansion of x.

Putting all pieces together

Theorem

If x is polynomial time random then x is normal in base β for all Pisot β.

Proof sketch

- Suppose $(x\beta^n)_{n\in\mathbb{N}}$ is not u.d. mod 1. Let $s = \beta$-expansion of x.
- By Bertrand's theorem, s is not distributed according to P_β.

Putting all pieces together

Theorem

If x is polynomial time random then x is normal in base β for all Pisot β.

Proof sketch

- Suppose $(x\beta^n)_{n\in\mathbb{N}}$ is not u.d. mod 1. Let $s = \beta$-expansion of x.
- By Bertrand's theorem, s is not distributed according to P_β.
- Consider (X_β, T) and use

Theorem

Let (X, T) be a Markov subshift and let P be a Markov measure with support X which is invariant and irreducible. Then $s \in X$ is distributed according to P iff no P-martingale generated by a DFA succeeds on s.

Putting all pieces together

Theorem

If x is polynomial time random then x is normal in base β for all Pisot β.

Proof sketch

- Suppose $(x\beta^n)_{n\in\mathbb{N}}$ is not u.d. mod 1. Let $s = \beta$-expansion of x.
- By Bertrand's theorem, s is not distributed according to P_β.
- (X_β, T) is not Markov, so we can't use

Theorem

Let (X, T) be a Markov subshift and let P be a Markov measure with support X which is invariant and irreducible. Then $s \in X$ is distributed according to P iff no P-martingale generated by a DFA succeeds on s.

Putting all pieces together

Theorem

If x is polynomial time random then x is normal in base β for all Pisot β.

Proof sketch

- Suppose $(x\beta^n)_{n\in\mathbb{N}}$ is not u.d. mod 1. Let $s = \beta$-expansion of x.
- By Bertrand's theorem, s is not distributed according to P_β.
- (X_β, T) is not Markov, so we can't use

Theorem

Let (X, T) be a Markov subshift and let P be a Markov measure with support X which is invariant and irreducible. Then $s \in X$ is distributed according to P iff no P-martingale generated by a DFA succeeds on s.

But (X_β, T) is sofic, and we can use

Another Theorem

The generalization of $\Leftarrow$ to sofic subshifts still holds.

Putting all pieces together

Theorem

If x is polynomial time random then x is normal in base β for all Pisot β.

Proof sketch

- Suppose $(x\beta^n)_{n\in\mathbb{N}}$ is not u.d. mod 1. Let $s = \beta$-expansion of x.
- By Bertrand's theorem, s is not distributed according to P_β.
- (X_β, T) is not Markov, so we can't use

  Theorem

  Let (X, T) be a Markov subshift and let P be a Markov measure with support X which is invariant and irreducible. Then $s \in X$ is distributed according to P iff no P-martingale generated by a DFA succeeds on s.

  But (X_β, T) is sofic, and we can use

  Another Theorem

  The generalization of $\Leftarrow$ to sofic subshifts still holds.

- There is a P_β-martingale f generated by a DFA which succeeds on s.

Putting all pieces together

Theorem

If x is polynomial time random then x is normal in base β for all Pisot β.

Proof sketch

- Suppose $(x\beta^n)_{n\in\mathbb{N}}$ is not u.d. mod 1. Let $s = \beta$-expansion of x.
- By Bertrand's theorem, s is not distributed according to P_β.
- (X_β, T) is not Markov, so we can't use

Theorem

Let (X, T) be a Markov subshift and let P be a Markov measure with support X which is invariant and irreducible. Then $s \in X$ is distributed according to P iff no P-martingale generated by a DFA succeeds on s.

But (X_β, T) is sofic, and we can use

Another Theorem

The generalization of $\Leftarrow$ to sofic subshifts still holds.

- There is a P_β-martingale f generated by a DFA which succeeds on s.
- Use that s and P_β are polytime computable to obtain, from f, a classical polytime martingale in base 2 which succeeds on the binary representation of x.

Thank you!