Computable absolutely normal numbers and discrepancies

Adrian Scheerer

Institute of Analysis and Number Theory
TU Graz

Prime Numbers and Automatic Sequences: Determinism and Randomness
Luminy

May 22nd, 2017

Analysis &
Number Theory
TU Graz

azt.tugraz.at

Let $b \geq 2$ be an integer. Let x be a real number and denote its base-b expansion by

$$x = \lfloor x \rfloor + 0.\epsilon_1 \epsilon_2 \epsilon_3 \ldots$$

with digits $0 \leq \epsilon_i \leq b - 1$.

Let $b \geq 2$ be an integer. Let x be a real number and denote its base-b expansion by

$$x = \lfloor x \rfloor + 0.\epsilon_1 \epsilon_2 \epsilon_3 \ldots$$

with digits $0 \leq \epsilon_i \leq b - 1$.

Definition

A real number x is *normal to base* $b \geq 2$ if all finite blocks of digits occur with the expected frequency in its base b expansion.

Let $b \geq 2$ be an integer. Let x be a real number and denote its base-b expansion by

$$x = \lfloor x \rfloor + 0.\epsilon_1\epsilon_2\epsilon_3\ldots$$

with digits $0 \leq \epsilon_i \leq b-1$.

Definition

A real number x is *normal to base* $b \geq 2$ if all finite blocks of digits occur with the expected frequency in its base b expansion.

For all k, for all digits $d_1, \ldots, d_k$,

$$\frac{1}{N}\#\{i \leq N : \epsilon_i\epsilon_{i+1}\ldots\epsilon_{i+k-1} = d_1\ldots d_k\} \longrightarrow \frac{1}{b^k}$$

as $N \to \infty$.

Introduction

Let $b \geq 2$ be an integer. Let x be a real number and denote its base-b expansion by

$$x = \lfloor x \rfloor + 0.\epsilon_1 \epsilon_2 \epsilon_3 \ldots$$

with digits $0 \leq \epsilon_i \leq b - 1$.

Definition

A real number x is *normal to base* $b \geq 2$ if all finite blocks of digits occur with the expected frequency in its base b expansion.

For all k, for all digits $d_1, \ldots, d_k$,

$$\frac{1}{N} \#\{i \leq N : \epsilon_i \epsilon_{i+1} \ldots \epsilon_{i+k-1} = d_1 \ldots d_k\} \longrightarrow \frac{1}{b^k}$$

as $N \to \infty$.

x is called *absolutely normal* if it is normal to all integer bases $b \geq 2$.

Introduction

◇ Almost all numbers are (absolutely) normal.
(Borel, 1909)

Introduction

- Almost all numbers are (absolutely) normal.
  (Borel, 1909)
- 0. 1 2 3 4 5 6 7 8 9 10 11 ... is normal to base 10.
  (Champernowne, 1933)

- Almost all numbers are (absolutely) normal.
  (Borel, 1909)
- 0. 1 2 3 4 5 6 7 8 9 10 11 . . . is normal to base 10.
  (Champernowne, 1933)
- 0. 2 3 5 7 11 13 17 . . . is normal to base 10.
  (Copeland/Erdős, 1946)

Introduction

- Almost all numbers are (absolutely) normal.
  (Borel, 1909)
- 0. 1 2 3 4 5 6 7 8 9 10 11 . . . is normal to base 10.
  (Champernowne, 1933)
- 0. 2 3 5 7 11 13 17 . . . is normal to base 10.
  (Copeland/Erdős, 1946)
- No algebraic number is known to be normal or not normal, nor is any arithmetical constant known to be normal or not normal.

- Almost all numbers are (absolutely) normal.
  (Borel, 1909)
- 0. 1 2 3 4 5 6 7 8 9 10 11 . . . is normal to base 10.
  (Champernowne, 1933)
- 0. 2 3 5 7 11 13 17 . . . is normal to base 10.
  (Copeland/Erdős, 1946)
- No algebraic number is known to be normal or not normal, nor is any arithmetical constant known to be normal or not normal.
- There is no easy example of an absolutely normal number.

Let the base $\beta > 1$ be a real number. Every real x can be represented in the form

$$\begin{aligned} x &= \lfloor x \rfloor + 0.\epsilon_1\epsilon_2\epsilon_3\ldots \\ &= \lfloor x \rfloor + \sum_{i=1}^{\infty} \epsilon_i \beta^{-i} \end{aligned}$$

where the digits ϵ_i are integers $0 \le \epsilon_i < \beta$ that are chosen in increasing order of i as large as possible.

A *Pisot number* is a real algebraic integer > 1, all of whose conjugates lie in the unit disk. Integers ≥ 2 are usually included in this definition.

A *Pisot number* is a real algebraic integer > 1, all of whose conjugates lie in the unit disk. Integers ≥ 2 are usually included in this definition.

There is a unique T_β-invariant ergodic probability measure μ_β on $[0,1)$ of maximum entropy that is equivalent to the Lebesgue-measure.

A *Pisot number* is a real algebraic integer > 1, all of whose conjugates lie in the unit disk. Integers ≥ 2 are usually included in this definition.

There is a unique T_β-invariant ergodic probability measure μ_β on $[0, 1)$ of maximum entropy that is equivalent to the Lebesgue-measure.

Definition

x is normal to base β, if $(T_\beta^n(x))_{n\geq 0}$ is uniformly distributed modulo 1 with respect to μ_β.

- There are various constructions of normal numbers to a given base β by concatenating strings.

Continued fractions

Any real number x has a continued fraction expansion of the form

$$x = [a_0; a_1, a_2, a_3 \ldots]$$

where $a_0 = \lfloor x \rfloor \in \mathbb{Z}$ and $a_i \in \mathbb{N}$ for $i \geq 1$.

Continued fractions

Any real number x has a continued fraction expansion of the form

$$x = [a_0; a_1, a_2, a_3 \ldots]$$

where $a_0 = \lfloor x \rfloor \in \mathbb{Z}$ and $a_i \in \mathbb{N}$ for $i \geq 1$.
The a_i are obtained from x via $a_i(x) = \lfloor 1/T_G^{i-1}(x) \rfloor$ where

$$T_G : [0,1) \to [0,1), \; x \mapsto \frac{1}{x} \text{ mod } 1 \text{ if } x > 0, \; \text{and } 0 \mapsto 0,$$

is the Gauss map.

Continued fractions

Any real number x has a continued fraction expansion of the form

$$x \;=\; [a_0; a_1, a_2, a_3 \ldots]$$

where $a_0 = \lfloor x \rfloor \in \mathbb{Z}$ and $a_i \in \mathbb{N}$ for $i \geq 1$.
The a_i are obtained from x via $a_i(x) = \lfloor 1/T_G^{i-1}(x) \rfloor$ where

$$T_G : [0,1) \to [0,1),\ x \mapsto \frac{1}{x} \text{ mod } 1 \text{ if } x > 0,\ \text{ and } 0 \mapsto 0,$$

is the Gauss map.
T_G possesses a unique invariant ergodic measure $\mu_G = \frac{1}{\log 2} \frac{dx}{1+x}$ of maximum entropy.

Continued fractions

Any real number x has a continued fraction expansion of the form

$$x \; = \; [a_0; a_1, a_2, a_3 \ldots]$$

where $a_0 = \lfloor x \rfloor \in \mathbb{Z}$ and $a_i \in \mathbb{N}$ for $i \geq 1$.
The a_i are obtained from x via $a_i(x) = \lfloor 1/T_G^{i-1}(x) \rfloor$ where

$$T_G : [0,1) \to [0,1), \; x \mapsto \frac{1}{x} \bmod 1 \text{ if } x > 0, \; \text{and } 0 \mapsto 0,$$

is the Gauss map.
T_G possesses a unique invariant ergodic measure $\mu_G = \frac{1}{\log 2} \frac{dx}{1+x}$ of maximum entropy.

Definition

x is called *continued fraction normal*, if $(T_G^n(x))_{n \geq 0}$ is uniformly distributed modulo 1 with respect to μ_G.

E.g., concatenate the partial quotients of
$1/2, 1/3, 2/3, 1/4, 2/4, 3/4, \ldots$ (Adler/Keane/Smorodinsky)

Ergodic theorem: almost all real numbers are normal.

Constructions of absolutely normal numbers

Ergodic theorem: almost all real numbers are normal.

Constructions of absolutely normal numbers have been given by Sierpinski, Turing, Schmidt, Levin, Becher/Figueira, Becher/Heiber/Slaman.

Constructions of absolutely normal numbers

Ergodic theorem: almost all real numbers are normal.

Constructions of absolutely normal numbers have been given by Sierpinski, Turing, Schmidt, Levin, Becher/Figueira, Becher/Heiber/Slaman.

There seems to be a trade-off between the time-complexity and convergence to normality ($D_N \to 0$) of these algorithms.

Constructions of absolutely normal numbers

Ergodic theorem: almost all real numbers are normal.

Constructions of absolutely normal numbers have been given by Sierpinski, Turing, Schmidt, Levin, Becher/Figueira, Becher/Heiber/Slaman.

There seems to be a trade-off between the time-complexity and convergence to normality ($D_N \to 0$) of these algorithms.

Becher/Heiber/Slaman: polynomial time, but $D_N = O(\frac{1}{\log N})$
Sierpinski, Lebesgue, Turing: double-exp. time, but $D_N = O(\frac{1}{N^\epsilon})$ for some small ϵ.

A string of digits ω of length n is called (ϵ, k)-*normal*, if every word d of length k appears at least $n(1-\epsilon)\mu(d)$ and at most $n(1+\epsilon)\mu(d)$ times in ω.

Some preliminaries

A string of digits ω of length n is called (ϵ, k)-*normal*, if every word d of length k appears at least $n(1-\epsilon)\mu(d)$ and at most $n(1+\epsilon)\mu(d)$ times in ω.

A real number x is called *simply normal* to base b, if all base-b digits of x appear with the same asymptotic frequency.

Absolute normality is equivalent to simple normality to all bases.

Idea:

- Compute a nested sequence of binary intervals by iteratively halving the previous interval and deciding which of the halves is 'best':
- do so by successively computing a number in $[0,1) \setminus B_N$ for N increasing with the step of the algorithm where B_N is an approximation to B, the set of 'bad' numbers.
- This will produce a number in $[0,1) \setminus B$, the set of all 'good' numbers.

B is the set of all non-(ϵ, k)-normal numbers.

Idea:

- Successively concatenate (ϵ, k)-normal words to an increasing set of bases *simultaneously*.
- Any concatenation of (ϵ, k)-normal words, subject to weak conditions, will be normal.
- Cylinder intervals should be well-behaved.

Need to show explicitly that there is an abundance of (ϵ, k)-normal words.

Theorem (Equipartition)

Let T be an ergodic transformation on a probability space $(X, \mathcal{B}, \mu)$. For any $\epsilon > 0$ there is an $n_0 = n_0(\epsilon)$ such that for all $n \geq n_0$ the set of cylinders of length n decomposes into two sets H and L such that

$$\mu(L) < \epsilon$$

and for any cylinder $c \in H$

$$\exp(-n(h(T) - \epsilon)) < \mu(c) < \exp(-n(h(T) + \epsilon)).$$

- Ergodicity: If $T^{-1}(A) = A$, then $\mu(A) \in \{0, 1\}$.
- $h(T)$ is the entropy of T.
- A cylinder of length n is a subset of $[0, 1)$ in which all numbers have the same first n digits.

Absolutely Pisot normal numbers

We call a real number *absolutely Pisot normal*, if it is normal to each base β that is a Pisot number.

We call a real number *absolutely Pisot normal*, if it is normal to each base β that is a Pisot number.

Theorem (with Manfred Madritsch and Robert Tichy)

There is an algorithm that uses only elementary operations to compute an absolutely Pisot normal number.

Absolutely Pisot normal numbers

We call a real number *absolutely Pisot normal*, if it is normal to each base β that is a Pisot number.

Theorem (with Manfred Madritsch and Robert Tichy)

There is an algorithm that uses only elementary operations to compute an absolutely Pisot normal number.

Proof:

- Becher/Heiber/Slaman-construction of choosing simultaneously to several bases long 'good' blocks of digits.
- Explicit estimate for (ϵ, k)-normal numbers.

Levin has also given such a construction using exponential sums estimates.

For β-expansions:

- ◇ The digits are independent, if one looks at two digits that are far enough away from each other.
- ◇ Admissible sequences are exactly sequences all of whose shifts are lexicographically strictly less than the *modified expansion* of 1.
- ◇ Inserting enough zeros in-between two words gives again an admissible word. ‘Enough’ can be made explicit and depends only on the base, not on the blocks.

Non-(ϵ, k)-normal numbers for β-expansions

Fix a string d of k digits in base β, let $X_i(x) = 1 - \mu_\beta(c(d))$ if d appears in x at i-th position, and $X_i(x) = -\mu_\beta(c(d))$ if not.

Non-(ϵ, k)-normal numbers for β-expansions

Fix a string d of k digits in base β, let $X_i(x) = 1 - \mu_\beta(c(d))$ if d appears in x at i-th position, and $X_i(x) = -\mu_\beta(c(d))$ if not.

Theorem (A. Siegel)

Let $X = X_1 + X_2 + \ldots + X_k$ be the sum of k possibly dependent random variables. Suppose that X_i, for $i = 1, 2, \ldots, k$, is the sum of n_i mutually independent random variables having values in the interval $[0, 1]$. Let $E[X_i] = n_i p_i$. Then for $a \geq 0$

$$P(X - E[X] \geq a) < \textit{two explicit exponential terms } (a, k, p_i, n_i)$$

Non-(ϵ, k)-normal numbers for β-expansions

Fix a string d of k digits in base β, let $X_i(x) = 1 - \mu_\beta(c(d))$ if d appears in x at i-th position, and $X_i(x) = -\mu_\beta(c(d))$ if not.

Theorem (A. Siegel)

Let $X = X_1 + X_2 + \ldots + X_k$ be the sum of k possibly dependent random variables. Suppose that X_i, for $i = 1, 2, \ldots, k$, is the sum of n_i mutually independent random variables having values in the interval $[0, 1]$. Let $E[X_i] = n_i p_i$. Then for $a \geq 0$

$$P(X - E[X] \geq a) < \textit{two explicit exponential terms } (a, k, p_i, n_i)$$

Lemma (Madritsch, S., Tichy)

Let β be a Pisot number. The μ_β-measure of the set of not (ϵ, k)-normal words of length n satisfies

$$\mu_\beta(B(n, \epsilon, k)) \leq 4\beta^k \beta^{-\eta n}$$

for $n \geq M + k$ with explicit $\eta > 0$ and M.

Absolutely continued fraction normal numbers

Theorem

There is an algorithm that uses only elementary operations to compute an absolutely normal number that is also continued fraction normal.

This gives a solution to a problem of Bugeaud and Queféllec .

Absolutely continued fraction normal numbers

Theorem

There is an algorithm that uses only elementary operations to compute an absolutely normal number that is also continued fraction normal.

This gives a solution to a problem of Bugeaud and Quefélec .

Proof:

- Sierpinski's construction.
- Explicit estimate for (ϵ, k)-normal numbers for continued fractions.

Absolutely continued fraction normal numbers

Theorem

There is an algorithm that uses only elementary operations to compute an absolutely normal number that is also continued fraction normal.

This gives a solution to a problem of Bugeaud and Queféllec .

Proof:

- Sierpinski's construction.
- Explicit estimate for (ϵ, k)-normal numbers for continued fractions.

Has already been greatly improved some weeks ago by Becher and Yuhjtman, who could adapt Becher, Heiber and Slaman's polynomial algorithm.
In particular, they used that $q_n(x) \sim e^{nL}$ a.e., where $L = \pi^2/(12\log(2))$.

Non-(ϵ, k)-normal numbers for continued fraction expansions

Fix a string $d_1 \dots d_k$ of k positive integers.

Let $X_i(x)$ be the normalized random variable that counts whether or not the string $d_1 \dots d_k$ appears in the continued fraction expansion of x at position i.

Non-(ϵ, k)-normal numbers for continued fraction expansions

Fix a string $d_1 \dots d_k$ of k positive integers.

Let $X_i(x)$ be the normalized random variable that counts whether or not the string $d_1 \dots d_k$ appears in the continued fraction expansion of x at position i.

The X_i are not independent, but they satisfy a mixing property that can be derived from mixing properties of the partial quotients a_i:

W. Philipp:
$|\mu_G(A \cap B) - \mu_G(A)\mu_G(B)| \leq \rho^n \mu_G(A)\mu_G(B)$ for all $A \in \sigma(a_1, \dots, a_k)$, $B \in \sigma(a_{k+n}, a_{k+n+1}, \dots)$ for some $0 < \rho < 0.8$.

Theorem (F. Merlevède, M. Peligrad, E. Rio)

Let $(X_i)_{i\geq 1}$ be a sequence of centered real-valued random variables bounded by a uniform constant M and with $\alpha_n(X_i)$ satisfying $\alpha_n \leq \exp(-2nc)$ for some positive c. Then there is an explicit positive constant C depending only on c such that for all $n \geq 4$ and $x \geq 0$

$$\mathbb{P}(|X_1 + \ldots + X_n| \geq x) \leq \exp\left(-\frac{Cx^2}{nM^2 + Mx(\log n)(\log\log n)}\right).$$

Theorem (F. Merlevède, M. Peligrad, E. Rio)

Let $(X_i)_{i\geq 1}$ be a sequence of centered real-valued random variables bounded by a uniform constant M and with $\alpha_n(X_i)$ satisfying $\alpha_n \leq \exp(-2nc)$ for some positive c. Then there is an explicit positive constant C depending only on c such that for all $n \geq 4$ and $x \geq 0$

$$\mathbb{P}(|X_1 + \ldots + X_n| \geq x) \leq \exp\left(-\frac{Cx^2}{nM^2 + Mx(\log n)(\log\log n)}\right).$$

Lemma

$$\mu_G(B_{CF}(\epsilon, d_1 \ldots d_k, n)) \leq \exp\left(-\eta_{CF}(\epsilon, d_1 \ldots d_k)\frac{n}{\log n}\right)$$

for some explicit $\eta_{CF}(\epsilon, \overrightarrow{d}) > 0$ and all $n \geq n_0 = 2(k+1)$.

This was only known explicitly with linear decay by Vandehey (not enough for this application).

A sequence $(x_n)_{n\geq 0}$ of real numbers is called *uniformly distributed modulo* 1 if for any interval $I \subseteq [0,1)$,

$$\frac{1}{N}\#\{n \leq N : x_n \bmod 1 \in I\} \longrightarrow \lambda(I)$$

as $N \to \infty$.

A sequence $(x_n)_{n\geq 0}$ of real numbers is called *uniformly distributed modulo* 1 if for any interval $I \subseteq [0,1)$,

$$\frac{1}{N}\#\{n \leq N : x_n \bmod 1 \in I\} \longrightarrow \lambda(I)$$

as $N \to \infty$.

Wall (1949):
x is normal to base b if and only if $(b^n x)_{n\geq 0}$ is uniformly distributed modulo 1.

Normal numbers and discrepancies

A sequence $(x_n)_{n\geq 0}$ of real numbers is called *uniformly distributed modulo* 1 if for any interval $I \subseteq [0,1)$,

$$\frac{1}{N}\#\{n \leq N : x_n \bmod 1 \in I\} \longrightarrow \lambda(I)$$

as $N \to \infty$.

Wall (1949):
x is normal to base b if and only if $(b^n x)_{n\geq 0}$ is uniformly distributed modulo 1.

The quantity

$$D_N(x_n) \;=\; \sup_{I\subseteq[0,1)} \left| \frac{1}{N}\#\{n \leq N : x_n \bmod 1 \in I\} - \lambda(I) \right|$$

is called the *discrepancy* of (x_n).

Results on discrepancy

- For N fixed: $\frac{1}{N} \leq D_N(x_n) \leq 1$.

Results on discrepancy

- For N fixed: $\frac{1}{N} \leq D_N(x_n) \leq 1$.
- W. Schmidt (1972):
  There is a positive absolute constant c such that for any sequence $D_N \geq c\frac{\log N}{N}$ holds for infinitely many N.

Results on discrepancy

- For N fixed: $\frac{1}{N} \leq D_N(x_n) \leq 1$.
- W. Schmidt (1972):
  There is a positive absolute constant c such that for any sequence $D_N \geq c\frac{\log N}{N}$ holds for infinitely many N.
- Schiffer (1986):
  The discrepancy of Champernowne's and Copeland-Erdős' numbers is $\Theta(\frac{1}{\log N})$.

Results on discrepancy

- For N fixed: $\frac{1}{N} \leq D_N(x_n) \leq 1$.
- W. Schmidt (1972):
  There is a positive absolute constant c such that for any sequence $D_N \geq c\frac{\log N}{N}$ holds for infinitely many N.
- Schiffer (1986):
  The discrepancy of Champernowne's and Copeland-Erdős' numbers is $\Theta(\frac{1}{\log N})$.
- Philipp (1974/75), Fukuyama (2013):
  for almost all x: $\limsup_{N\to\infty} \frac{D_N(b^n x)N^{1/2}}{(\log\log N)^{1/2}} = c(b) > 0$.

Results on discrepancy

- For N fixed: $\frac{1}{N} \leq D_N(x_n) \leq 1$.
- W. Schmidt (1972):
  There is a positive absolute constant c such that for any sequence $D_N \geq c\frac{\log N}{N}$ holds for infinitely many N.
- Schiffer (1986):
  The discrepancy of Champernowne's and Copeland-Erdős' numbers is $\Theta(\frac{1}{\log N})$.
- Philipp (1974/75), Fukuyama (2013):
  for almost all x: $\limsup_{N\to\infty} \frac{D_N(b^n x)N^{1/2}}{(\log\log N)^{1/2}} = c(b) > 0$.
- Levin (1979, 1999):
  For $b \geq 2$, he constructed x with $D_N(b^n x) = O(\frac{(\log N)^2}{N})$, and x such that $D_N(b^n x) = O_b(\frac{(\log N)^3}{N^{1/2}})$ for all $b \geq 2$.

Absolutely normal numbers of low discrepancy

Theorem (with Verónica Becher and Theodore Slaman)

There is an algorithm that uses only elementary operations to compute an absolutely normal number x *in triple-exp. time, but with* $D_N(b^n x) = O(\frac{\sqrt{\log \log N}}{\sqrt{N}})$*, for all* $b \geq 2$.

Absolutely normal numbers of low discrepancy

Theorem (with Verónica Becher and Theodore Slaman)

There is an algorithm that uses only elementary operations to compute an absolutely normal number x in triple-exp. time, but with $D_N(b^n x) = O(\frac{\sqrt{\log \log N}}{\sqrt{N}})$, for all $b \geq 2$.

Proof:

- Combine Sierpinski's construction with estimates by Philipp on the discrepancy of sequences of the form $(b^n x)_{n \geq 0}$.

Thank you for your attention!