# On Normal Numbers

Verónica Becher

Universidad de Buenos Aires and CONICET
Laboratoire INFINIS

Talk at Université Paris Diderot, July 12, 2013

# Normal numbers

A *base* is an integer greater than or equal to 2.

**Definition (Borel, 1909)**

Let $x$ be a real number.

- $x$ is *simply normal to base b* if in the expansion of $x$ in base $b$, $(x)_b$, each digit occurs with limiting frequency equal to $1/b$.
- $x$ is *normal to base b* if $x$ is simply normal to every base $b^j$, for every positive integer $j$.
- $x$ is *absolutely normal* if it is normal to every base.

# Existence of absolutely normal numbers

Theorem (Borel 1909)

*Almost all real numbers are absolutely normal.*

# Normality to different bases

Problem

*How does normality to one base relate to normality to another base?*

Simple normality to base $s^m$ implies simple normality to base $s$.
But not conversely....

Except for one elementary condition, there is no relation between normality to one base and normality to another.

# Multiplicative independence

Definition

For positive integers $s_1$ and $s_2$, we say $s_1$ and $s_2$ are *multiplicatively dependent* if each is a rational power of the other.

Examples

2and 4 are multiplicatively dependent.
2 and 6 are multiplicatively independent.

Theorem (Maxfield 1953)

*If $s_1$ and $s_2$ are multiplicatively dependent bases, then, for any real $x$, $x$ is normal to base $s_1$ if and only if it is normal to base $s_2$.*

Hence, $x$ is absolutely normal if and only if it is normal to some representative of each multiplicative dependence equivalence class.

# Normality to different bases

**Theorem (Schmidt 1961/62)**

*For any given set of bases, closed under multiplicative dependence, there are real numbers normal to every base from the given set and not normal to any base in its complement.*

# Five questions

Question one

*For the multiplicatively independent bases to which a number is normal, are the discrepancy functions pairwise independent?*

Question two (asked by Kechris 1994, Ditzen 1994)

*Does the set of bases for which a number is normal play a distinguished role among its other arithmetical properties?*

Question three (asked by Brown, Moran and Pearce 1985)

*Does Schmidt's theorem hold denying simple normality?*

Question four (various)

*What are the conditions on the set of bases to which a number is simply normal?*

Question five (various)

*Can we compute an absolutely normal number in polynomial time?*

# Five answers

# Normality as uniform distribution modulo one

**Definition**

The *discrepancy* of a sequence $(x_1, \ldots, x_n)$ of real numbers in $[0,1]$ is

$$D(x_1, \ldots, x_n) = \sup_{0 \le u < v \le 1} \left| \frac{\#\{j : 1 \le j \le n, u \le x_j < v\}}{n} - (v-u) \right|.$$

The fractional part of a real $x$ is $\{x\}$. To consider normality of $x$ to base $s$,

$$(\{s^j x\} : 0 \le j < \infty).$$

A real $x$ is normal to base $s$ iff $(\{s^j x\} : 0 \le j < \infty)$ is uniformly distributed in $[0,1]$

**Theorem (Wall 1949)**

*A real number $x$ is normal to base $s$ iff* $\lim_{n\to\infty} D(\{s^j x\} : 0 \le j \le n) = 0$.

Thus, for every $0 \le u < v \le 1$, $\lim_{n\to\infty} \frac{\#\{j : 1 \le j \le n, u \le \{s^j x\} < v\}}{n} = (v-u)$.

# Normal numbers and Weyl's criterion

**Theorem** (Weyl's Criterion)

*A sequence of reals* $(x_j : 1 \leq j < \infty)$ *is uniformly distributed modulo one if, and only if, for every complex-valued 1-periodic continuous function* $f$*,*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{j=1}^{n} f(x_j) = \int_0^1 f(x)dx.$$

*That is, if and only if, for every non-zero integer* $t$*,* $\lim_{n\to\infty} \frac{1}{n} \sum_{j=1}^{n} e^{2\pi\, i\, t\, x_j} = 0.$

Thus, a real number $x$ is normal to base $s$ iff for every non-zero integer $t$,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} e^{2\pi\, i\, t\, s^j x} = 0.$$

# Effective Weyl criterion

**Theorem** (LeVeque 1965)

$$D(x_1, \ldots, x_n) \leq \left( \frac{6}{\pi^2} \sum_{t=1}^{\infty} \frac{1}{t^2} \left| \frac{1}{n} \sum_{j=1}^{n} e^{2\pi\, i\, t\, x_j} \right|^2 \right)^{\frac{1}{3}}.$$

**Lemma**

*For any positive real $\epsilon$ there is a finite set of integers $T$ and a positive real $\delta$ such that for any sequence of reals $(x_1, \ldots, x_n)$,*

*if for all $t \in T$,* $\frac{1}{n^2} \left| \sum_{j=1}^{n} e^{2\pi\, i\, t\, x_j} \right|^2 < \delta$ *then* $\quad D(x_1, \ldots, x_n) < \epsilon.$

*Furthermore, such $T$ and $\delta$ can be computed from $\epsilon$.*

# A version of the Cantor set

Definition

For $s$ an integer greater than 2, let $\tilde{s}$ denote $s-1$ if $s$ is odd and denote $s-2$ if $s$ is even.

Theorem (Schmidt 1960)

*Consider the fractal subset of $[0,1)$ consisting of the real numbers whose expansion in base $s$ is given by sequences of digits in $\{0,1,\ldots,\tilde{s}-1\}$, with its uniform measure. Almost every element of this set is normal to every base multiplicatively independent to $s$ (and not normal to base $s$).*

# A discrepancy floor

A real number in an $\tilde{s}$-fractal omits the last digit (or the last two digits) in its base $s$ expansion and so can not be simply normal to base $s$.

**Lemma**

*Let $n$ and $m$ be positive integers and $I$ an interval such that $n \geq \lceil 2m/\mu(I) \rceil$. Suppose that $(x_1, \dots x_n)$ is a sequence of reals of length $n$ and that for all $m \leq j \leq n$, $x_j \notin I$. Then,*

$$D(I, (x_1, \dots x_n)) = \left| \frac{\#\{j : 1 \leq j \leq n, x_j \in I\}}{n} - \mu(I) \right| \geq \mu(I)/2$$

# Question one

For the multiplicatively independent bases to which a number is normal, are the discrepancy functions pairwise independent?

**Theorem** (Becher and Slaman 2013)

*Fix a base $s$. There is a computable $f : \mathbb{N} \to \mathbb{Q}$ monotonically decreasing to 0 such that for any $g : \mathbb{N} \to \mathbb{Q}$ monotonically decreasing to 0 there is an absolutely normal real number $x$ whose discrepancy for base $s$ eventually dominates $g$ and whose discrepancy for each base multiplicatively independent to $s$ is eventually dominated by $f$. Furthermore, $x$ is computable from $g$.*

# Question two

Is the set of bases to which a number is normal independent of other arithmetical properties?

Recall Borel hierarchy for subsets of the real numbers is the stratification of the $\sigma$-algebra generated by the open sets with the usual interval topology.

When we restrict to intervals with rational endpoints and computable countable unions and intersections, we obtain the effective Borel hierarchy.

Asked first by Kechris 1994.

**Theorem** (Ki and Linton 1994)

*The set of real numbers that are normal to any fixed base is* $\mathbf{\Pi}^0_3$*-complete.*

**Theorem** (Becher, Heiber and Slaman 2013)

*The set of real numbers that are absolutely normal is* $\Pi^0_3$*-complete.*

Confirming a conjecture of Ditzen 1994,

**Theorem** (Becher and Slaman 2013)

*The set of real numbers that are normal to some base is* $\Sigma^0_4$*-complete.*

# A fixed point

Recall that a formula in the arithmetic hierarchy involves only quantification over integers.

**Theorem** (Becher and Slaman 2013)

*For any $\Pi^0_3$ formula $\phi$ in second order arithmetic there is a computable real $x$ such that for $s$ in the set of minimal representatives of the multiplicative dependence equivalence classes, $x$ is normal to base $s$ if and only if $\phi(x, s)$ is true.*

# Question three

Does Schmidt's theorem hold denying simple normality?

Addressing the issue raised by Brown, Moran and Pearce 1985,

**Theorem** (Becher and Slaman 2013)

*For any given set of bases, closed under multiplicative dependence, there are real numbers normal to every base from the given set and not simply normal to any base in its complement. Furthermore, such reals can be obtained computably from the given set of bases.*

# Question four

What are the conditions on the set of bases to which a number is simply normal?

**Theorem** (Long 1957)

*If real number is simply normal to base $s^m$ for infinitely many exponents $m$, then it is normal to base $s$ and so simply normal to base $s^m$ for every $m$.*

**Theorem** (Hertling 2002)

*Simple normality to base $s_1$ implies simple normality to base $s_2$ if, and only if, $s_1$ is a power of $s_2$.*

Let $\widetilde{\mathbb{N}}$ the minimal representatives of the multiplicatively dependence classes.

**Theorem** (Becher, Bugeaud and Slaman 2013)

*Let $M$ be a function that assigns to each $s \in \widetilde{\mathbb{N}}$ a set $M(s)$ of positive integers such that if $m \in M(s)$ then so are all of its divisors and if $M(s)$ is infinite then it is equal to $\mathbb{N}$. There is a real number $x$ such that for every base $s \in \widetilde{\mathbb{N}}$, $x$ is simply normal to base $s^m$ if and only if $m \in M(s)$.*

# Question five

Can we compute an absolutely normal number in polynomial time?

**Problem** (Borel 1909)

*Give one example of an absolutely normal number.*

First constructions by Lebesgue and independently by Sierpiński, 1917.
M. Levin constructed absolutely normal numbers with low discrepancy in 1979.

**Theorem** (Turing ∼1938, see Becher, Figueira and Picchi 2007)

*There is a computable absolutely normal number.*

Other computable instances Schmidt 1961/1962; also Becher and Figueira 2002.

# Absolutely normal numbers in just above quadratic time

**Theorem** (Becher, Heiber and Slaman 2013)

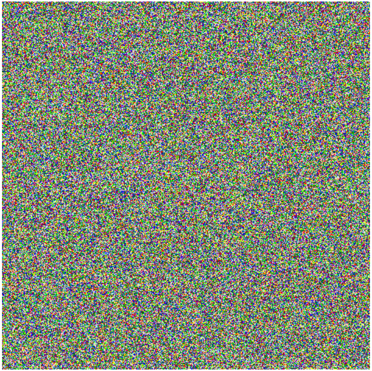
*Suppose* $f : \mathbb{N} \to \mathbb{N}$ *is a computable non-decreasing unbounded function. There is an algorithm to compute an absolutely normal number* $x$ *such that, for any base* $b$*, the algorithm outputs the first* $i$ *digits in* $(x)_b$ *after* $O(f(i)\, i^2)$ *elementary operations.*

Lutz and Mayordomo (2013) and also Figueira and Nies (2013) have another argument for an absolutely normal number in polynomial time, based on polynomial-time martingales.

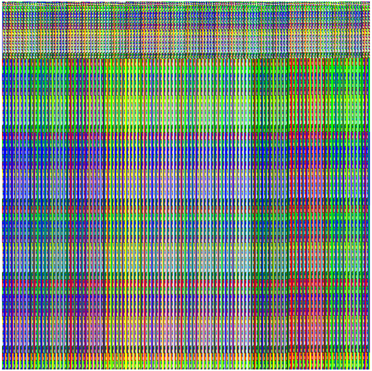
# The output of our algorithm in base 10

Programmed by Martin Epszteyn

0.403129054200380913237142838082705910276511677762418977511089636 6...



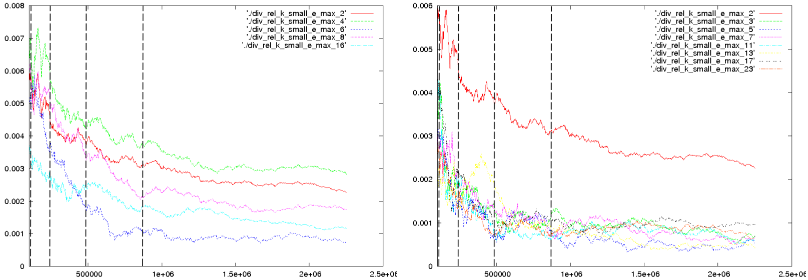
First 250000 digits output by the algorithm
Plotted in 500x500 pixeles, 10 colors



First 250000 digits of Champernowne
Plotted in 500x500 pixeles, 10 colors

Algorithm with parameters $t_i = (3 * \log(i)) + 3$; $\epsilon_i = 1/t_i$ Initial values $t_1 = 3$; $\epsilon_1 = 1$.
First extension in base 2 is of length $k = 405$. Then $k$ increases only when necessary.

# The output of our algorithm in each base




Left: Discrepancy for powers of 2, normalized by expected frequency.
Right: Discrepancy for prime digits, normalized by expected frequency.

On normal numbers, Paris, July 12, 2013.

# Recall the Borel hierarchy for subsets of the real numbers

Recall Borel hierarchy for subsets of the real numbers is the stratification of the $\sigma$-algebra generated by the open sets with the usual interval topology.

$A$ is $\boldsymbol{\Sigma}^0_1$ iff $A$ is open. $A$ is $\boldsymbol{\Pi}^0_1$ iff $A$ is closed.
$A$ is $\boldsymbol{\Sigma}^0_{n+1}$ iff it is countable union of $\boldsymbol{\Pi}^0_n$ sets. $A$ is $\boldsymbol{\Pi}^0_{n+1}$ iff it is a countable intersection of $\boldsymbol{\Sigma}^0_n$ sets.

When we restrict to intervals with rational endpoints and computable countable unions and intersections, we obtain the effective Borel hierarchy.

$A$ is $\Sigma^0_n$ (respectively $\Pi^0_n$) iff membership in that set is definable by a formula in of second-order arithmetic which is $\Sigma^0_n$ (respectively $\Pi^0_n$).

$A$ is hard for an (effective) Borel class if every set in the class is reducible to $A$ by a continuous (computable) map. $A$ is complete in class if it is hard for this class and belongs to the class.

Since computable maps are continuous, proofs of hardness in the effective hierarchy often yield proofs of hardness in general by relativization. This is the case in our work.