On Normal Numbers

Verónica Becher

Universidad de Buenos Aires and CONICET
Laboratoire Franco-Argentine INFINIS

Dagstuhl Seminar "Duality in Computer Science", July 28 – August 2, 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 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.

Counterexamples

- 0.01010010001000010000010000...
  is not simply normal to base 2.
- 0.01010101010101010101010101...
  is simply normal to base 2, but not simply normal to base 4.
- for each rational number $q \in \mathbb{Q}$ there is a base b such that the expansion of q in base b ends with all zeros; hence, q is not simply normal to base b.

The problem is still open

Theorem (Borel 1909)

Almost all real numbers are absolutely normal.

Problem (Borel 1909)

Give an example of an absolutely normal number.

Conjecture (Borel 1954)

Irrational algebraic numbers are absolutely normal.

Normal to a given base

Theorem (Champernowne 1933)

0.12345678910111213141516 ... *is normal to base* 10*.*

Theorem (Bailey, Borwein 2012)

Stoneham number $\alpha_{2,3} = \sum_{n \geq 1} \frac{1}{3^n 2^{3^n}}$ *is normal to base* 2 *but not to base* 6*.*

Part I : finite automata

Normality and finite automata

Definition

A deterministic *transducer* is a tuple $T = \langle Q, A, B, \delta, q_0 \rangle$, where

- Q is a finite set of states,
- A and B are the input and output alphabets, respectively,
- $\delta : Q \times A \to B^* \times Q$ is the transition function,
- $q_0 \in Q$ is the starting state.

If $\delta(p, a) = \langle v, q \rangle$ we write $p \xrightarrow{a|v} q$.
An *infinite run* is $p_0 \xrightarrow{a_1|v_1} p_1 \xrightarrow{a_2|v_2} p_2 \xrightarrow{a_3|v_3} p_3 \cdots$ is accepting if $p_0 = q_0$.
This is the Büchi acceptance condition where all states are accepting.

Definition

A sequence $x = a_1 a_2 a_3 \cdots$ is *compressible* by a transducer if and only if its accepting run $q_0 \xrightarrow{a_1|v_1} q_1 \xrightarrow{a_2|v_2} q_2 \xrightarrow{a_3|v_3} q_3 \cdots$ satisfies

$$\liminf_{n \to \infty} \frac{|v_1 v_2 \cdots v_n| \log |B|}{n \qquad \log |A|} < 1.$$

Normality and finite automata

Theorem (Schnorr, Stimm 1971 + Dai, Lathrop, Lutz, Mayordomo 2004)

A real is normal to base b if, and only if, its expansion in base b is incompressible by injective finite transducers.

Huffman 1959 calls them lossless compressors.

A direct proof of the above theorem Becher and Heiber, 2012.

Theorem (Becher, Carton, Heiber 2013)

Non-deterministic bounded-to-one transducers, even if augmented with a fixed number of counters, can not compress normal infinite words.

Theorem (Boasson, personal communication 2012)

Non-deterministic puhdown transducers can compress normal infinite words.

Question

What is the least powerful machine that compressess normal infinite words?
Can deterministic pushdown automata compress normal infinite words?

Normality preservation and finite automata

Definition

Let $x = a_1 a_2 a_3 \cdots$ be an infinite word over alphabet A.

Let $L \subseteq A^*$. The infinite word obtained by *prefix-selection* of x by L is $a_{p(1)} a_{p(2)} \cdots$, where $p(j)$ is the j-th in sorted $\{i \ : \ a_1 a_2 \cdots a_{i-1} \in L\}$.

Let $X \subseteq A^\omega$. The infinite word obtained by *suffix-selection* of x by X is $a_{s(1)} a_{s(2)} \cdots$, where $s(j)$ is the j-th in sorted $\{i : a_{i+1} a_{i+2} \cdots \in X\}$.

Theorem (Agafonov1968)

Prefix selection by a regular set of finite words preserves normality.

Theorem (Becher, Carton, Heiber 2013)

Suffix selection by a regular set of infinite words preserves normality.

Normality preservation and finite automata

Theorem (Becher, Carton, Heiber 2013)

Two sided selectors do not preserve normality.

Theorem (Merkle, Reimann 2006)

Neither deterministic one-counter sets (sets recognized by pushdown automata with a unary stack) nor linear sets (sets recognized by one-turn pushdown automata) preserve normality.

Question

What is the least powerful selection that does not preserve normality?

Part II : simple normality

Normality to different bases

Definition

Two positive integers *multiplicatively dependent* if each is a rational power of the other.

Examples:
2 and 8 are multiplicatively dependent; 2 and 6 are multiplicatively independent.

Theorem (Maxfield 1953)

If s and t are multiplicatively dependent bases, then, for any real x, x is normal to base s if and only if it is normal to base t.

Normality to different bases

Theorem (Schmidt 1961)

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.

Theorem (Becher, 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.

Simple normality to different bases

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*, hence simply normal to base* s^m *for every* m*.*

Theorem (Hertling 2002)

Simple normality to base s *implies simple normality to base* t *if and only if* s *is a power of* t*. Moreover, for* s *and* t *both greater than* 2*, such that* s *is not a power of* t*, the set of numbers which are simply normal to base* s*, but not simply normal to base* t*, is uncountable.*

Simple normality to different bases

Let $\mathcal{S}$ be the set of numbers that are not pefect powers, that is

$$\mathcal{S} = \{2, 3, 5, 6, 7, 10, 11, \ldots\}$$

Theorem (Becher, Bugeaud, Slaman 2013)

Let M be a function from $\mathcal{S}$ to sets of positive integers such that, for each s in $\mathcal{S}$, if m is in $M(s)$ then each divisor of m is in $M(s)$ and if $M(s)$ is infinite then it is equal to the set of all positive integers.

There is a real number x, which is computable from M, such that, for every s in $\mathcal{S}$, x is simply normal to base s^m if and only if m is in $M(s)$.

Moreover, the set of real numbers x such that, for every integer s in $\mathcal{S}$, x is simply normal to base s^m if and only if m is in $M(s)$, has full Hausdorff dimension.

Normal numbers and Weyl's criterion

Theorem (Wall 1949)

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

Theorem (Weyl's Criterion)

A real number x is normal to base s if and only if for every non-zero integer t,

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

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 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.

Part III: Surprise

Constructions of absolutely normal numbers

Back to 1909.

Problem (Borel 1909)

Give an example of an absolutely normal number.

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

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

There is a computable absolutely normal number.

Other computable instances Schmidt 1961; also Becher, Figueira 2002.

Absolutely normal numbers in just above quadratic time

Theorem (Becher, Heiber, Slaman 2013)

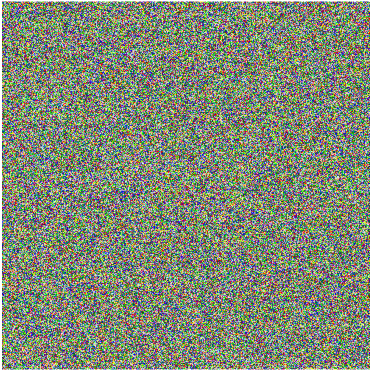
Suppose $f : \mathbb{N} \to \mathbb{N}$ is a computable non-decreasing unbounded function. There is an algorithm to compute an absolutely normal number x such that, for any base b, the algorithm outputs the first n digits in of its expansion after $O(f(n)\, n^2)$ elementary operations.

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

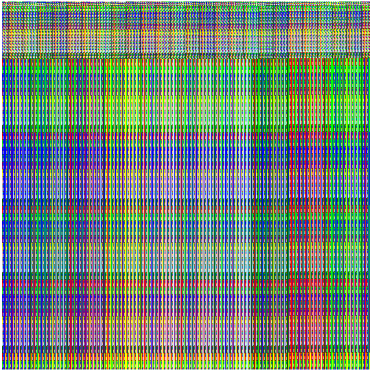
The output of our algorithm in base 10

Programmed by Martin Epszteyn

0.4031290542003809132371428380827059102765116777624189775110896366...



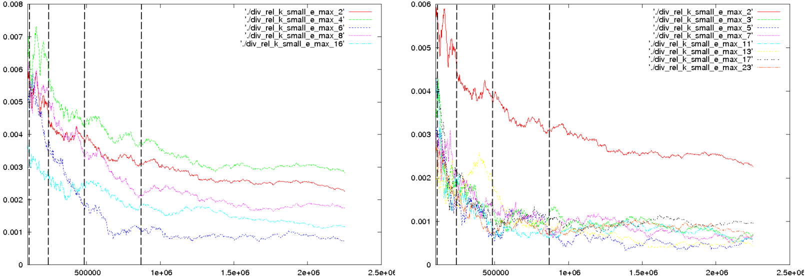
First 250000 digits output by the algorithm
Plotted in 500x500 pixeles, 10 colors



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.

Open questions

Question

What is the least powerful automata that compressess normal infinite words? Can deterministic pushdown automata compress normal infinite words?

Question

What is the least powerful selection automata that des not preserve normality?

Question

Is it possible to construct (absolutely) normal numbers with some other mathematical property?

Question

Is there a a polynomial time algorithm that computes a number that is simply normal to a given set of bases (according to the Theorem) and not simply normal to the bases in the complement?