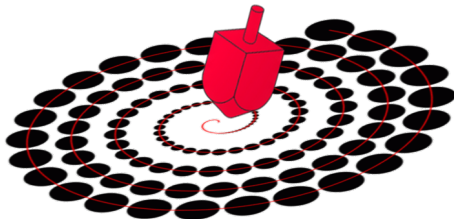


# Four Lectures On Normal Numbers

Verónica Becher, Santiago Figueira,  
Pablo Ariel Heiber and Theodore A. Slaman

University of Buenos Aires and University of California, Berkeley



Buenos Aires Semester  
Computability, Complexity and Randomness  
March 2013

# Equivalent Definitions of Normality and Selected Theorems

This story starts in 1909, when Émile Borel defined normality.

# Notation

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

A *digit* in base  $b$  is an element in  $\{0, \dots, b - 1\}$ ,

A *block* in base  $b$  is a finite sequence of digits in base  $b$ .

The length of a block  $w$  is  $|w|$ .

The subblock of  $w$  from position  $i$  to  $j$ , where  $1 \leq i \leq j \leq |w|$ , is  $w[i..j]$ .

$\text{occ}(w, u) = \#\{i : w[i..i + |u| - 1] = u\}$ .

For each real number  $\xi$  in the unit interval and for each base  $b$  we consider the unique *expansion of  $\xi$  in base  $b$* ,  $a_1 a_2 a_3 \dots$  such that

$\xi = \sum_{i=1}^{\infty} a_i b^{-i}$  where  $a_i$  is digit in base  $b$  and  $a_i < b - 1$  infinitely many times.

# Definition of normality

The expansion in base  $b$  of a real  $\xi$  is denoted by  $(\xi)_b$ .

## Definition (Borel 1909)

A real number  $\xi$  is *simply normal to base  $b$*  if for each digit  $d$  in base  $b$

$$\lim_{n \rightarrow \infty} \text{occ}((\xi)_b[1..n], d)/n = 1/b.$$

$\xi$  is *normal to base  $b$*  if each of  $\xi, b\xi, b^2\xi \dots$  is simply normal to  $b^i$ , for  $i \geq 1$ .

$\xi$  is *absolutely normal* if it is normal to every base  $b$ .

# Definition of normality

## Definition (Borel 1914)

$\xi$  is *normal* to base  $b$  if for every block  $u$  in base  $b$  of every length

$$\lim_{n \rightarrow \infty} \text{occ}((\xi)_b[1..n], u) / n = 1/b^{|u|}.$$

$\xi$  is *absolutely normal* if it is normal to every base  $b$ .

# Definition of normality

## Definition (Pillai 1940)

$\xi$  is *normal to base  $b$*  if it is simply normal to the bases  $b^i$ , for every  $i \geq 1$ .

$\xi$  is *absolutely normal* if it is simply normal to every base.

# The still open question

## Theorem (Borel 1909)

*Almost all real numbers are absolutely normal.*

We will prove it by giving a Martin Löf test that covers every non absolutely normal number.



# The still open question

## Theorem (Borel 1909)

*Almost all real numbers are absolutely normal.*

We will prove it by giving a Martin Löf test that covers every non absolutely normal number.

## Problem

*Give one example of an absolutely normal number.*

# More than 100 years

## Conjecture (Borel 1950)

*Irrational algebraic numbers are absolutely normal.*

First constructions by Lebesgue and independently Sierpiński, 1917.

M. Levin 1979 absolutely normal numbers with low discrepancy.

Bugeaud 2002 proved the existence of Liouville absolutely normal numbers.

# More than 100 years

## Conjecture (Borel 1950)

*Irrational algebraic numbers are absolutely normal.*

First constructions by Lebesgue and independently Sierpiński, 1917.

M. Levin 1979 absolutely normal numbers with low discrepancy.

Bugeaud 2002 proved the existence of Liouville absolutely normal numbers.

## Theorem (Turing ~1938)

*There is a computable absolutely normal number.*

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

# More than 100 years

## Conjecture (Borel 1950)

*Irrational algebraic numbers are absolutely normal.*

First constructions by Lebesgue and independently Sierpiński, 1917.

M. Levin 1979 absolutely normal numbers with low discrepancy.

Bugeaud 2002 proved the existence of Liouville absolutely normal numbers.

## Theorem (Turing ~1938)

*There is a computable absolutely normal number.*

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

## Theorem (Mayordomo 2013; Figueira Nies 2013; Becher Heiber Slaman 2013)

*A polynomial time algorithm for absolutely normal numbers.*

The respective time complexities are  $n^2 \log^* n$ ,  $n^4$  and  $n^2 f(n)$  for any nondecreasing unbounded  $f$ .

# Not absolutely normal

## Definition

A real number is *absolutely abnormal* if it is not normal to any base.

## Theorem (Martin 2001)

*There are absolutely abnormal numbers.*

# Not absolutely normal

## Definition

A real number is *absolutely abnormal* if it is not normal to any base.

## Theorem (Martin 2001)

*There are absolutely abnormal numbers.*

## Theorem (particular case Cassels 1959, Schmidt 1960)

*There are numbers not simply normal to a given base  $b$  but normal to all other bases multiplicatively independent to  $b$ .*

## Theorem (Schmidt 1961/62)

*Let  $S$  be any set of bases. There are numbers normal to each base in  $S$  and not normal to each base multiplicatively independent to the elements in  $S$ .*

Improvement of Schmidt's theorem denying simple normal Becher Slaman 2013

# Normal to a given base

Theorem (Champernowne 1933)

$0,123456789101112131415161718192021222324 \dots$  is normal to base ten.

# Normality in five different formulations

1. Combinatorial (Borel's original definition and equivalent forms)
2. Uniform distribution of sequences modulo one
3. Weyl's criterion
4. Incompressibility by lossless finite automata
5. Polynomial martingales



# Normality in five different formulations

1. Combinatorial (Borel's original definition and equivalent forms)
2. Uniform distribution of sequences modulo one
3. Weyl's criterion
4. Incompressibility by lossless finite automata
5. Polynomial martingales

Normality and randomness tests?

# Normal numbers and uniform distribution modulo one

## Definition

Let  $N$  be a positive integer and  $\xi_1, \dots, \xi_N$  be reals between 0 and 1. The *discrepancy* of the sequence  $(\xi_1, \dots, \xi_N)$  is

$$D(\xi_1, \dots, \xi_N) = \sup_{0 \leq u < v \leq 1} \left| \frac{\#\{n : 1 \leq n \leq N, u \leq \xi_n < v\}}{N} - (v - u) \right|.$$

The fractional part of the real number  $\xi$  will be denoted  $\{\xi\}$ .

Let  $b$  be a base and consider the sequences

$$(\{b^j \xi\} : j \geq 0)$$

## Theorem (Wall 1949)

Let  $b$  be a base. A real number  $\xi$  is normal to base  $b$  if and only if

$$\lim_{N \rightarrow \infty} D(\{b^j \xi\} : 0 \leq j < N) = 0.$$

# Normal numbers and Weyl's criterion

## Theorem (Weyl's Criterion)

A sequence  $(\xi_n : n \geq 1)$  is uniformly distributed modulo one if and only if for every complex-valued 1-periodic continuous function  $f$ ,

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{j=1}^N f(\xi_n) = \int_0^1 f(x) dx.$$

That is, if and only if for every non-zero integer  $t$ ,  $\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{j=1}^N e^{2\pi i t \xi_j} = 0$

Thus,  $\xi$  is normal to base  $b$  iff for every non-zero  $t$

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{j=0}^{N-1} e^{2\pi i t b^j \xi} = 0.$$

# Effective Weyl criterion

Theorem (LeVeque 1965)

$$D(\xi_1, \dots, \xi_N) \leq \left( \frac{6}{\pi^2} \sum_{t=1}^{\infty} \frac{1}{t^2} \left| \frac{1}{N} \sum_{j=1}^N e^{2\pi i t \xi_j} \right|^2 \right)^{\frac{1}{3}}.$$

Lemma (Becher Slaman 2013)

For any positive real  $\varepsilon$  there is a finite set of integers  $T$  and a positive real  $\delta$  such that for any  $(\xi_1, \dots, \xi_N)$ , if for all  $t \in T$ ,  $\frac{1}{N^2} \left| \sum_{j=1}^N e^{2\pi i t \xi_j} \right|^2 < \delta$  then  $D(\xi_1, \dots, \xi_N) < \varepsilon$ . Furthermore, such  $T$  and  $\delta$  can be computed from  $\varepsilon$ .

# Normal numbers and incompressibility

## Definition (Huffman 1959)

A lossless finite-state compressor is an ordinary finite automata augmented with an output transition function such that the automata input-output behavior is injective.

## Theorem (Schnorr Stimm 1972 + Dai Lathrop Lutz Mayordomo 2004; Becher and Heiber 2013)

*A real number is normal to a given integer base if, and only if, its expansion expressed in that base is incompressible by lossless finite-state compressors.*

# Normal numbers and martingales

A martingale for alphabet of  $b$  symbols is such that for all blocks  $w$  in base  $b$

$$d(w) = b^{-1} \sum_{a \in \{0, \dots, (b-1)\}} d(wa).$$

The martingale  $d$  succeeds on a sequence  $w \in b^\omega$  if  $\limsup_{n \rightarrow \infty} d(w[1..n]) = \infty$ .

**Theorem (Schnorr Stimm 1972 + Dai Lathrop Lutz Mayordomo 2004)**

*$\xi$  is normal to base  $b$  if and only if no finite-state martingale succeeds on  $\xi$ .*

**Theorem (Schnorr 1971)**

*If no quadratic-time martingale succeeds on the expansion of  $\xi$  in base 2 then  $\xi$  is normal to base 2.*

**Theorem (Hitchcock Mayordomo 2013; Figuera Nies 2013)**

*If no polynomial-time martingale succeeds on the expansion of  $\xi$  in base 2 then  $\xi$  is absolutely normal.*

# Normal numbers and randomness tests

Theorem (Turing ~1938)

*Schnorr randomness implies absolute normality.*

# Normal numbers and randomness tests

**Theorem (Turing ~1938)**

*Schnorr randomness implies absolute normality.*

We give a family of Martin Löf-tests. For each base  $b$  and each dyadic rational  $\varepsilon$ ,  $(S(\varepsilon, b)_k)_{k \geq 1}$  is a uniformly c.e. sequence of sets of intervals with rational endpoints whose measure is computably bounded and goes to zero.

For fixed parameters  $b, \varepsilon$ , and for each  $k$ ,  $S(b, \varepsilon)_k$  is the c.e. set of intervals with  $b$ -adic rational endpoints. The initial segment of length  $k$  of expansion in base  $b$  of these rational endpoints contains, according to  $\varepsilon$ , too many or too few occurrences of some digit.



## There are only a few bad blocks (the Key Lemma)

Fix a base  $b$  and a block  $u$  of length  $\ell$ .

The expected number of occurrences of  $u$  in any block of length  $N$  is  $N/b^\ell$ .

## There are only a few bad blocks (the Key Lemma)

Fix a base  $b$  and a block  $u$  of length  $\ell$ .

The expected number of occurrences of  $u$  in any block of length  $N$  is  $N/b^\ell$ .

Suppose  $w$  is a block of length  $N$ . If  $u$  occurs in  $w$  more than  $N/b^\ell + \varepsilon N$  times, or less than  $N/b^\ell - \varepsilon N$  times, then  $w$  is a bad block for  $u$ .

## There are only a few bad blocks (the Key Lemma)

Fix a base  $b$  and a block  $u$  of length  $\ell$ .

The expected number of occurrences of  $u$  in any block of length  $N$  is  $N/b^\ell$ .

Suppose  $w$  is a block of length  $N$ . If  $u$  occurs in  $w$  more than  $N/b^\ell + \varepsilon N$  times, or less than  $N/b^\ell - \varepsilon N$  times, then  $w$  is a bad block for  $u$ .

**Lemma** (extends Hardy Wright 1938)

Fix base  $b$ , a block  $u$  of length  $\ell$  and a length  $N$  such that  $N > \ell$ .

For any real  $\varepsilon$  such that  $6/\lfloor N/\ell \rfloor \leq \varepsilon \leq 1/b^\ell$

$$\sum_{\substack{i < N/b^\ell - \varepsilon N \text{ or} \\ i > N/b^\ell + \varepsilon N}} \text{the number of blocks of length } N \\ \text{with exactly } i \text{ occurrences of } w \leq 2 b^N b^{2\ell-2} e^{-b^\ell \varepsilon^2 N/6\ell}.$$

Hint: the number of blocks of length  $N$  with exactly  $i$  occurrences of a given *digit* is  $\binom{N}{i} (b-1)^{k-i}$ .

# Normal numbers and randomness tests

Fix  $b$  and  $\varepsilon$ . Let  $k_0$  be the least such that the Key Lemma holds for  $\ell = 1$  and  $\varepsilon$  and  $b$  as given.

For each  $k \geq k_0$ ,

$$S(b, \varepsilon)_k = \bigcup_{N > k} \{w \in b^N : |\text{occ}(w, d) - N/b| > \varepsilon N \text{ for some digit } d \text{ in base } b\}$$

# Normal numbers and randomness tests

Fix  $b$  and  $\varepsilon$ . Let  $k_0$  be the least such that the Key Lemma holds for  $\ell = 1$  and  $\varepsilon$  and  $b$  as given.

For each  $k \geq k_0$ ,

$$S(b, \varepsilon)_k = \bigcup_{N > k} \{w \in b^N : |\text{occ}(w, d) - N/b| > \varepsilon N \text{ for some digit } d \text{ in base } b\}$$

$$\mu(S(b, \varepsilon)_k) \leq \sum_{N > k} 2 b e^{-b\varepsilon^2 N/6} \leq \int_k^\infty 2be^{-b\varepsilon^2 N/6} dN = 12\varepsilon^{-2} e^{-b\varepsilon^2 k/6}.$$

## Normal numbers and randomness tests

Fix  $b$  and  $\varepsilon$ . Let  $k_0$  be the least such that the Key Lemma holds for  $\ell = 1$  and  $\varepsilon$  and  $b$  as given.

For each  $k \geq k_0$ ,

$$S(b, \varepsilon)_k = \bigcup_{N > k} \{w \in b^N : |\text{occ}(w, d) - N/b| > \varepsilon N \text{ for some digit } d \text{ in base } b\}$$

$$\mu(S(b, \varepsilon)_k) \leq \sum_{N > k} 2 b e^{-b\varepsilon^2 N/6} \leq \int_k^\infty 2be^{-b\varepsilon^2 N/6} dN = 12\varepsilon^{-2} e^{-b\varepsilon^2 k/6}.$$

If a real  $\xi$  is *not* absolutely normal then there is some base  $b$  and some  $\varepsilon$  such that  $\xi \in \bigcap_{k \geq k_0} S(b, \varepsilon)_k$ .

# No Martin-Löf test for absolute normality exactly

# No Martin-Löf test for absolute normality exactly

**Theorem (Ki Linton 1994)**

*Fix base  $b$ . The set of real numbers normal to base  $b$  is  $\Pi_3^0$ -complete.*

Thus, for every Martin-Löf test  $(S_k)_k$

$$\bigcap_k S_k \neq \{\xi \in (0, 1) : \xi \text{ is not normal to base } b\}$$



# No Martin-Löf test for absolute normality exactly

**Theorem (Ki Linton 1994)**

*Fix base  $b$ . The set of real numbers normal to base  $b$  is  $\Pi_3^0$ -complete.*

Thus, for every Martin-Löf test  $(S_k)_k$

$$\bigcap_k S_k \neq \{\xi \in (0, 1) : \xi \text{ is not normal to base } b\}$$

**Theorem (Becher Heiber Slaman 2013)**

*The set of real numbers that are absolutely normal is  $\Pi_3^0$ -complete.*

# No Martin-Löf test for absolute normality exactly

**Theorem (Ki Linton 1994)**

*Fix base  $b$ . The set of real numbers normal to base  $b$  is  $\Pi_3^0$ -complete.*

Thus, for every Martin-Löf test  $(S_k)_k$

$$\bigcap_k S_k \neq \{\xi \in (0, 1) : \xi \text{ is not normal to base } b\}$$

**Theorem (Becher Heiber Slaman 2013)**

*The set of real numbers that are absolutely normal is  $\Pi_3^0$ -complete.*

As conjectured by Achim Ditzen,

**Theorem (Becher Slaman 2013)**

*The set of real numbers that are normal to some base is  $\Sigma_4^0$ -complete.*

# A convenient characterization of normality

## Theorem (Bugeaud 2012)

*A real  $\xi$  is normal to base  $b$  if and only if there is a positive constant  $C$  such that, for every length  $\ell$  and for every block  $u$  in base  $b$  of length  $\ell$ ,*

$$\limsup_{N \rightarrow \infty} \frac{\text{occ}((\xi)_b[1..N], u)}{N} \leq \frac{C}{b^\ell}.$$

# Champernowne's number is normal to base ten

We will prove for every length  $\ell$ , every block  $u$  in base  $b$  of length  $\ell$

$$\limsup_{N \rightarrow \infty} \frac{\text{occ}(1\dots N, u)}{N} \leq \frac{2 \cdot 10}{10^\ell}.$$

We consider the segments

$$1\dots 9 \quad 10\dots 99 \quad 100\dots 999 \quad 1000\dots 9999 \quad 10^i\dots 9^{i+1}\dots$$

Define  $(S_i)_{i \geq 0}$  where  $S_i = 10^i\dots 9^{i+1}$  and its length is  $L_i = (i+1) \cdot 9 \cdot 10^i$ .

Champernowne's number is normal to base ten

# Champernowne's number is normal to base ten

How many times does the digit 1 occur in  $S_i$ ?

# Champernowne's number is normal to base ten

How many times does the digit 1 occur in  $S_i$ ?

$S_i$	
123456789	1
101112131...21...31...41.....99	10 +9
100...999 :	100 +9 10 +9 10
$10^3..9^4 :$	$10^3$ +9 10 +9 10 +9 10
$10^i ...9^{i+1}$	$10^i$ + $i$ 9 10

Since  $\ell = 1$  this is,

$$10^{i+1-\ell} + (i + 1 - \ell) 9 10^{i-\ell}$$

# Champernowne's number is normal in base ten

For  $i \geq 0$ ,  $S_i = 10^i \dots 9^{i+1}$  with length  $L_i = (i + 1) 9 \cdot 10^i$



# Champernowne's number is normal in base ten

For  $i \geq 0$ ,  $S_i = 10^i \dots 9^{i+1}$  with length  $L_i = (i + 1) 9 \cdot 10^i$

Suppose  $|u| = \ell$ . How many times  $u$  occurs in  $S_i = 10^i \dots 9^{i+1}$ ?

# Champernowne's number is normal in base ten

For  $i \geq 0$ ,  $S_i = 10^i \dots 9^{i+1}$  with length  $L_i = (i + 1) 9 \cdot 10^i$

Suppose  $|u| = \ell$ . How many times  $u$  occurs in  $S_i = 10^i \dots 9^{i+1}$ ?

Case not divided.

# Champernowne's number is normal in base ten

For  $i \geq 0$ ,  $S_i = 10^i \dots 9^{i+1}$  with length  $L_i = (i + 1) 9 \cdot 10^i$

Suppose  $|u| = \ell$ . How many times  $u$  occurs in  $S_i = 10^i \dots 9^{i+1}$ ?

Case not divided.

If  $u$  does not start with 0 then  $u$  occurs

$$10^{i+1-\ell} + (i + 1 - \ell) 9 \cdot 10^{i-\ell}$$

# Champernowne's number is normal in base ten

For  $i \geq 0$ ,  $S_i = 10^i \dots 9^{i+1}$  with length  $L_i = (i+1) 9 \cdot 10^i$

Suppose  $|u| = \ell$ . How many times  $u$  occurs in  $S_i = 10^i \dots 9^{i+1}$ ?

Case not divided.

If  $u$  does not start with 0 then  $u$  occurs

$$10^{i+1-\ell} + (i+1-\ell) 9 \cdot 10^{i-\ell}$$

If  $u$  starts with 0, it occurs just  $(i+1-\ell) 9 \cdot 10^{i-\ell}$ .

# Champernowne's number is normal in base ten

For  $i \geq 0$ ,  $S_i = 10^i \dots 9^{i+1}$  with length  $L_i = (i + 1) 9 \cdot 10^i$

Suppose  $|u| = \ell$ . How many times  $u$  occurs in  $S_i = 10^i \dots 9^{i+1}$ ?

Case not divided.

If  $u$  does not start with 0 then  $u$  occurs

$$10^{i+1-\ell} + (i + 1 - \ell) 9 \cdot 10^{i-\ell}$$

If  $u$  starts with 0, it occurs just  $(i + 1 - \ell) 9 \cdot 10^{i-\ell}$ .

Case divided.

# Champernowne's number is normal in base ten

For  $i \geq 0$ ,  $S_i = 10^i \dots 9^{i+1}$  with length  $L_i = (i + 1) 9 10^i$

Suppose  $|u| = \ell$ . How many times  $u$  occurs in  $S_i = 10^i \dots 9^{i+1}$ ?

Case not divided.

If  $u$  does not start with 0 then  $u$  occurs

$$10^{i+1-\ell} + (i + 1 - \ell) 9 10^{i-\ell}$$

If  $u$  starts with 0, it occurs just  $(i + 1 - \ell) 9 10^{i-\ell}$ .

Case divided.

$u$  occurs at most  $\ell - 1$  times the number of terms in the segment:

$$(\ell - 1) 9 10^i$$

# Champernowne's number is normal in base ten

For  $i \geq 0$ ,  $S_i = 10^i \dots 9^{i+1}$  with length  $L_i = (i + 1) 9 \cdot 10^i$ .

## Champernowne's number is normal in base ten

For  $i \geq 0$ ,  $S_i = 10^i \dots 9^{i+1}$  with length  $L_i = (i+1) 9 \cdot 10^i$ .

$$\begin{aligned} \text{occ}(1..9^k, u) &\leq \text{occurrences of } u \text{ undivided} + \text{occurrences of } u \text{ divided} \\ &\leq \left( \sum_{i=0}^k 10^{i+1-\ell} + (i+1-\ell) 9 \cdot 10^{i-\ell} \right) + \left( \sum_{i=0}^k (\ell-1) 9 \cdot 10^i \right) \\ &\leq \left( 10^{-\ell} \sum_{i=0}^k L_i \right) + \left( 10^{-\ell} (10 - 9\ell) \sum_{i=0}^k 10^i \right) + \left( (\ell-1) 9 \sum_{i=0}^k 10^i \right) \end{aligned}$$



## Champernowne's number is normal in base ten

For  $i \geq 0$ ,  $S_i = 10^i \dots 9^{i+1}$  with length  $L_i = (i+1) 9 \cdot 10^i$ .

$$\begin{aligned} \text{occ}(1..9^k, u) &\leq \text{occurrences of } u \text{ undivided} + \text{occurrences of } u \text{ divided} \\ &\leq \left( \sum_{i=0}^k 10^{i+1-\ell} + (i+1-\ell) 9 \cdot 10^{i-\ell} \right) + \left( \sum_{i=0}^k (\ell-1) 9 \cdot 10^i \right) \\ &\leq \left( 10^{-\ell} \sum_{i=0}^k L_i \right) + \left( 10^{-\ell} (10-9\ell) \sum_{i=0}^k 10^i \right) + \left( (\ell-1) 9 \sum_{i=0}^k 10^i \right) \end{aligned}$$

In case  $\ell = 1$ , there are no divided occurrences, so  $(\ell-1)$  is 0

$$\frac{\text{occ}(1..9^k, u)}{|1..9^k|} = \frac{\text{occ}(1..9^k, u)}{\sum_{i=0}^k L_i} \leq 10^{-\ell} + 10^{-\ell} = 2 \cdot 10^{-\ell}$$

## Champernowne's number is normal in base ten

For  $i \geq 0$ ,  $S_i = 10^i \dots 9^{i+1}$  with length  $L_i = (i+1) 9 \cdot 10^i$ .

$$\begin{aligned} \text{occ}(1..9^k, u) &\leq \text{occurrences of } u \text{ undivided} + \text{occurrences of } u \text{ divided} \\ &\leq \left( \sum_{i=0}^k 10^{i+1-\ell} + (i+1-\ell) 9 \cdot 10^{i-\ell} \right) + \left( \sum_{i=0}^k (\ell-1) 9 \cdot 10^i \right) \\ &\leq \left( 10^{-\ell} \sum_{i=0}^k L_i \right) + \left( 10^{-\ell} (10-9\ell) \sum_{i=0}^k 10^i \right) + \left( (\ell-1) 9 \sum_{i=0}^k 10^i \right) \end{aligned}$$

In case  $\ell = 1$ , there are no divided occurrences, so  $(\ell-1)$  is 0

$$\frac{\text{occ}(1..9^k, u)}{|1..9^k|} = \frac{\text{occ}(1..9^k, u)}{\sum_{i=0}^k L_i} \leq 10^{-\ell} + 10^{-\ell} = 2 \cdot 10^{-\ell}$$

In case  $\ell > 1$ ,  $(10-9\ell)$  is negative and for each  $\ell$  there is  $k_0$  such that for  $k \geq k_0$

$$\frac{\text{occ}(1..9^k, u)}{|1..9^k|} = \frac{\text{occ}(1..9^k, u)}{\sum_{i=0}^k L_i} \leq 10^{-\ell} + \frac{(\ell-1) 9}{k+1} \leq 2 \cdot 10^{-\ell}$$

## Champernowne's number is normal in base ten

For  $i \geq 0$ ,  $S_i = 10^i \dots 9^{i+1}$  with length  $L_i = (i+1) 9 \cdot 10^i$ .

$$\begin{aligned} \text{occ}(1..9^k, u) &\leq \text{occurrences of } u \text{ undivided} + \text{occurrences of } u \text{ divided} \\ &\leq \left( \sum_{i=0}^k 10^{i+1-\ell} + (i+1-\ell) 9 \cdot 10^{i-\ell} \right) + \left( \sum_{i=0}^k (\ell-1) 9 \cdot 10^i \right) \\ &\leq \left( 10^{-\ell} \sum_{i=0}^k L_i \right) + \left( 10^{-\ell} (10-9\ell) \sum_{i=0}^k 10^i \right) + \left( (\ell-1) 9 \sum_{i=0}^k 10^i \right) \end{aligned}$$

In case  $\ell = 1$ , there are no divided occurrences, so  $(\ell-1)$  is 0

$$\frac{\text{occ}(1..9^k, u)}{|1..9^k|} = \frac{\text{occ}(1..9^k, u)}{\sum_{i=0}^k L_i} \leq 10^{-\ell} + 10^{-\ell} = 2 \cdot 10^{-\ell}$$

In case  $\ell > 1$ ,  $(10-9\ell)$  is negative and for each  $\ell$  there is  $k_0$  such that for  $k \geq k_0$

$$\frac{\text{occ}(1..9^k, u)}{|1..9^k|} = \frac{\text{occ}(1..9^k, u)}{\sum_{i=0}^k L_i} \leq 10^{-\ell} + \frac{(\ell-1) 9}{k+1} \leq 2 \cdot 10^{-\ell}$$

Thus, for each  $\ell$  there is  $k_0$  such that for all  $k \geq k_0$ ,  $\frac{\text{occ}(1..9^k, u)}{|1..9^k|} \leq 2 \cdot 10^{-\ell}$ .

## Champernowne's number is normal in base ten

Consider an initial segment  $S^*$  of  $S_{k-1}$  such that the length of  $S^*$  is a multiple of  $k$ .

The last  $k$  digits of  $S^*$ ,  $m_{k-1} \dots m_0$ , correspond to the largest element in the specification of  $S^*$ . Note,  $m_{k-1}$  can be any non-zero digit and the other any digit.

Since  $S^* = 10^{k-1} \dots m_{k-1} \dots m_0$ ,  $|S^*| = k \left( (m_{k-1} - 1)10^{k-1} + \sum_{h=0}^{k-2} m_h 10^h \right)$ .

Consider a block  $u$  of length  $\ell$ .

Case  $u$  occurs divided in  $S^*$ .

Clearly  $\text{occ}(S^*, u) < (\ell - 1) m_{k-1} 10^{k-1}$ .

when  $k$  is large enough  $\frac{(\ell - 1) m_{k-1} 10^{k-1}}{|S^*|} < 10^{-\ell}$ .

Case  $u$  occurs undivided in  $S^*$ .

We count the number of blocks having  $u$  at fixed position  $j$ , for  $1 \leq j \leq k - \ell + 1$

# Champernowne's number is normal in base ten

Fix some  $j$  such that  $1 \leq j \leq k - \ell + 1$ .

We count how many blocks can have  $u$  at position  $j$ .

positions	1..... $(j-1)$	$j$ ..... $j+\ell-1$	$j+\ell$ ..... $k$
block	prefix	$u_1 \dots u_\ell$	suffix
maximum	$m_{k-1} \dots m_{k-(j-1)}$	$m_{k-j} \dots m_{k-j-\ell+1}$	$m_{k-j-\ell} \dots m_0$

The number of possible prefixes is at most

$$1 + (m_{k-1} - 1)10^{j-2} + \sum_{h=k-j+1}^{k-2} m_h 10^{h+j-k-1}.$$

The number of possible suffixes is at most

$$10^{k-j-\ell+1}.$$

## Champernowne's number is normal in base ten

We now consider all possible positions  $j = 1, 2, \dots, k - \ell + 1$ . The number of undivided occurrences of  $u$  in  $S^*$  is at most.

$$\begin{aligned} & 10^{k-\ell} + 10^{k-\ell-1}(1 + (m_{k-1} - 1)) + \\ & \sum_{j=3}^{k-\ell+1} 10^{k-j-\ell+1} \left( 1 + (m_{k-1} - 1)10^{j-2} + \sum_{h=k-j+1}^{k-2} m_h 10^{h+j-k-1} \right) \\ & \leq 10^{-\ell} \left( (1 + 10^{-1})10^k + (m_{k-1} - 1)10^{k-1} \right) + \\ & 10^{-\ell} \left( (k - \ell)(m_{k-1} - 1)10^{k-1} + \sum_{h=\ell}^{k-2} (h - \ell + 1)m_h 10^h \right) \end{aligned}$$

$$\text{Recall } S^* = 10^{k-1} \dots m_{k-1} \dots m_0 \quad |S^*| = k \left( (m_{k-1} - 1)10^{k-1} + \sum_{h=0}^{k-2} m_h 10^h \right).$$

Hence, the ratio of the number of undivided occurrences of  $u$  in  $S^*$  by the length of  $S^*$  is less than  $10 \cdot 10^{-\ell} + 10^{-\ell}$ .

# Champernowne's number is normal in base ten

Now, suppose that  $S$  is an initial segment of the Champernowne sequence. We view  $S$  as the concatenation of  $S_0, S_1, \dots, S_{k-2}, S^*$ , and a possible final sequence of length less than  $k$ .

$$\text{occ}(S, u) \leq \sum_{i=0}^{k-1} \text{occ}(S_i, u) + \text{occ}(S^*, u) + k$$

$$\frac{\text{occ}(S, u)}{|S|} \leq 2 \cdot 10^{-\ell} + (10 \cdot 10^{-\ell} + 10^{-\ell} + 10^{-\ell}) + 10^{-\ell} \leq 20 \cdot 10^{-\ell}.$$

# Proof of the limsup theorem

## Theorem (Bugeaud 2012)

*A real  $\xi$  is normal to base  $b$  if and only if there is a positive constant  $C$  such that for every block length  $\ell$  and for every block  $u$  in base  $b$  of length  $\ell$ ,*

$$\limsup_{N \rightarrow \infty} \frac{\text{occ}((\xi)_b[1..N], u)}{N} \leq \frac{C}{b^\ell}.$$



# Proof of the limsup theorem

## Theorem (Bugeaud 2012)

*A real  $\xi$  is normal to base  $b$  if and only if there is a positive constant  $C$  such that for every block length  $\ell$  and for every block  $u$  in base  $b$  of length  $\ell$ ,*

$$\limsup_{N \rightarrow \infty} \frac{\text{occ}((\xi)_b[1..N], u)}{N} \leq \frac{C}{b^\ell}.$$

The implication left to right is direct from the definition of normality.

# Proof of the limsup theorem

## Theorem (Bugeaud 2012)

*A real  $\xi$  is normal to base  $b$  if and only if there is a positive constant  $C$  such that for every block length  $\ell$  and for every block  $u$  in base  $b$  of length  $\ell$ ,*

$$\limsup_{N \rightarrow \infty} \frac{\text{occ}((\xi)_b[1..N], u)}{N} \leq \frac{C}{b^\ell}.$$

The implication left to right is direct from the definition of normality.

We prove the implication from right to left.

Fix  $b$ ,  $\xi$  and  $C$ , and assume the hypothesis. To show that  $\xi$  is normal to base  $b$  it suffices to prove that  $\xi$  is simply normal to base  $b^r$ , for each  $r \geq 1$ .

# Proof of the limsup theorem

Fix exponent  $r$  and a digit  $d$  in base  $b^r$ .

We give an upper bound of  $\text{occ}((\xi)_{b^r}[1..N], d)$ .

By hypothesis, for  $N$  sufficiently large,

given a block $u_r$	of length $r$ in base $b$ ,	$\text{occ}((\xi)_b[1..N], u_r)$	$< 2CN/b^r$
given a block $u_{rk}$	of length $rk$ in base $b$ ,	$\text{occ}((\xi)_b[1..N], u_{rk})$	$< 2CN/b^{rk}$
given a block $\hat{u}_k$	of length $k$ in base $b^r$ ,	$\text{occ}((\xi)_{b^r}[1..N], u_k)$	$< 2CNr/(b^r)^k$ .

# Proof of the limsup theorem

Let block size  $k = b^r n$ , where  $n$  will be determined at the end of the proof.

# Proof of the limsup theorem

Let block size  $k = b^r n$ , where  $n$  will be determined at the end of the proof.

The number of blocks of length  $k$  in the first  $N$  digits of  $\xi$  in base  $b^r$  is  $N/k$  (we consider non-overlapping blocks because we consider a single digit  $d$ ).

We classify them in **good blocks for  $d$**  and **bad blocks for  $d$** , for  $\varepsilon = k^{-1/3}$ .

# Proof of the limsup theorem

$\text{occ}((\xi)_{b^r}[1..N], d)$  is at most

#bad blocks for  $d \times \text{max occurrences of each bad block} \times \text{block size}$

+

all blocks  $\times$  the expected number of occurrences per block  $+ \varepsilon$  block size

# Proof of the limsup theorem

$\text{occ}((\xi)_{b^r}[1..N], d)$  is at most

#bad blocks for  $d \times \text{max occurrences of each bad block} \times \text{block size}$

+

all blocks  $\times$  the expected number of occurrences per block  $+ \varepsilon$  block size

$$\begin{aligned}\text{occ}((\xi)_{b^r}[1..N], d) &\leq (\text{\#bad blocks for } d) \frac{2CNr}{(b^r)^k} k + \frac{N}{k} \left( \frac{k}{b^r} + \varepsilon k \right) \\ &\leq 2(b^r)^k e^{-b^r \varepsilon^2 k/6} \frac{2CNr}{(b^r)^k} k + \frac{N}{b^r} (1 + \varepsilon) \\ &= 4Cr k e^{-(b^r)^{4/3} n^{1/3}/6} N + \frac{N}{b^r} (1 + \varepsilon)\end{aligned}$$

where the last equality uses  $k = b^r n$  and  $\varepsilon = k^{-1/3}$ .

# Proof of the limsup theorem

$\text{occ}((\xi)_{b^r}[1..N], d)$  is at most

#bad blocks for  $d \times \text{max occurrences of each bad block} \times \text{block size}$

+

all blocks  $\times$  the expected number of occurrences per block  $+ \varepsilon$  block size

$$\begin{aligned}\text{occ}((\xi)_{b^r}[1..N], d) &\leq (\text{\#bad blocks for } d) \frac{2CNr}{(b^r)^k} k + \frac{N}{k} \left( \frac{k}{b^r} + \varepsilon k \right) \\ &\leq 2(b^r)^k e^{-b^r \varepsilon^2 k/6} \frac{2CNr}{(b^r)^k} k + \frac{N}{b^r} (1 + \varepsilon) \\ &= 4Cr k e^{-(b^r)^{4/3} n^{1/3}/6} N + \frac{N}{b^r} (1 + \varepsilon)\end{aligned}$$

where the last equality uses  $k = b^r n$  and  $\varepsilon = k^{-1/3}$ .

Let  $n$  be such that  $4Cr k e^{-(b^r)^{4/3} n^{1/3}/6} N < \varepsilon \frac{N}{b^r}$ .



# Proof of the limsup theorem

$\text{occ}((\xi)_{b^r}[1..N], d)$  is at most

#bad blocks for  $d \times$  max occurrences of each bad block  $\times$  block size

+

all blocks  $\times$  the expected number of occurrences per block  $+ \varepsilon$  block size

$$\begin{aligned}\text{occ}((\xi)_{b^r}[1..N], d) &\leq (\text{\#bad blocks for } d) \frac{2CNr}{(b^r)^k} k + \frac{N}{k} \left( \frac{k}{b^r} + \varepsilon k \right) \\ &\leq 2(b^r)^k e^{-b^r \varepsilon^2 k/6} \frac{2CNr}{(b^r)^k} k + \frac{N}{b^r} (1 + \varepsilon) \\ &= 4Cr k e^{-(b^r)^{4/3} n^{1/3}/6} N + \frac{N}{b^r} (1 + \varepsilon)\end{aligned}$$

where the last equality uses  $k = b^r n$  and  $\varepsilon = k^{-1/3}$ .

Let  $n$  be such that  $4Cr k e^{-(b^r)^{4/3} n^{1/3}/6} N < \varepsilon \frac{N}{b^r}$ .

Then,  $\text{occ}((\xi)_{b^r}[1..N], d) < \frac{N}{b^r} (1 + 2\varepsilon)$ .

Hence,  $\limsup_{N \rightarrow \infty} \frac{\text{occ}((\xi)_{b^r}[1..N], d)}{N} \leq b^{-r}$ .

# Proof of the limsup theorem

$\text{occ}((\xi)_{b^r}[1..N], d)$  is at most

#bad blocks for  $d \times$  max occurrences of each bad block  $\times$  block size

+

all blocks  $\times$  the expected number of occurrences per block  $+ \varepsilon$  block size

$$\begin{aligned}\text{occ}((\xi)_{b^r}[1..N], d) &\leq (\text{\#bad blocks for } d) \frac{2CNr}{(b^r)^k} k + \frac{N}{k} \left( \frac{k}{b^r} + \varepsilon k \right) \\ &\leq 2(b^r)^k e^{-b^r \varepsilon^2 k/6} \frac{2CNr}{(b^r)^k} k + \frac{N}{b^r} (1 + \varepsilon) \\ &= 4Cr k e^{-(b^r)^{4/3} n^{1/3}/6} N + \frac{N}{b^r} (1 + \varepsilon)\end{aligned}$$

where the last equality uses  $k = b^r n$  and  $\varepsilon = k^{-1/3}$ .

Let  $n$  be such that  $4Cr k e^{-(b^r)^{4/3} n^{1/3}/6} N < \varepsilon \frac{N}{b^r}$ .

Then,  $\text{occ}((\xi)_{b^r}[1..N], d) < \frac{N}{b^r} (1 + 2\varepsilon)$ .

Hence,  $\limsup_{N \rightarrow \infty} \frac{\text{occ}((\xi)_{b^r}[1..N], d)}{N} \leq b^{-r}$ .

This holds for every digit  $d$  in base  $b^r$  and  $\sum_{d=0}^{b^r-1} \text{occ}((\xi)_{b^r}[1..N], d) = N$ .

# Proof of the limsup theorem

$\text{occ}((\xi)_{b^r}[1..N], d)$  is at most

#bad blocks for  $d \times$  max occurrences of each bad block  $\times$  block size

+

all blocks  $\times$  the expected number of occurrences per block  $+$   $\varepsilon$  block size

$$\begin{aligned}\text{occ}((\xi)_{b^r}[1..N], d) &\leq (\text{\#bad blocks for } d) \frac{2CNr}{(b^r)^k} k + \frac{N}{k} \left( \frac{k}{b^r} + \varepsilon k \right) \\ &\leq 2(b^r)^k e^{-b^r \varepsilon^2 k/6} \frac{2CNr}{(b^r)^k} k + \frac{N}{b^r} (1 + \varepsilon) \\ &= 4Cr k e^{-(b^r)^{4/3} n^{1/3}/6} N + \frac{N}{b^r} (1 + \varepsilon)\end{aligned}$$

where the last equality uses  $k = b^r n$  and  $\varepsilon = k^{-1/3}$ .

Let  $n$  be such that  $4Cr k e^{-(b^r)^{4/3} n^{1/3}/6} N < \varepsilon \frac{N}{b^r}$ .

Then,  $\text{occ}((\xi)_{b^r}[1..N], d) < \frac{N}{b^r} (1 + 2\varepsilon)$ .

Hence,  $\limsup_{N \rightarrow \infty} \frac{\text{occ}((\xi)_{b^r}[1..N], d)}{N} \leq b^{-r}$ .

This holds for every digit  $d$  in base  $b^r$  and  $\sum_{d=0}^{b^r-1} \text{occ}((\xi)_{b^r}[1..N], d) = N$ .

Hence,  $\xi$  is simply normal to base  $b^r$ .

## Bonus Track: Turing's effective null set

We define first a Martin Lőf test, uniformly in the parameter  $k$ .

$$S_k = \bigcup_{n \geq 0} S_{k,n}$$

## Bonus Track: Turing's effective null set

We define first a Martin Lőf test, uniformly in the parameter  $k$ .

$$S_k = \bigcup_{n \geq 0} S_{k,n}$$

$$S_{k,0} = \emptyset$$

$S_{k,n+1}$  add to  $S_{k,n}$  the points that are **not** candidates to be normal, due to an initial segment of their expansions in some base.

## Bonus Track: Turing's effective null set

We define first a Martin L\"of test, uniformly in the parameter  $k$ .

$$S_k = \bigcup_{n \geq 0} S_{k,n}$$

$$S_{k,0} = \emptyset$$

$S_{k,n+1}$  add to  $S_{k,n}$  the points that are **not** candidates to be normal, due to an initial segment of their expansions in some base.

$$S_{k,n} = \bigcup_{2 \leq b \leq B} \bigcup_{1 \leq \ell \leq L} \bigcup_{u \in \ell^*} \{w \in N^* : |\text{occ}(w, u) - N/b^\ell| > \varepsilon N\}$$

## Bonus Track: Turing's effective null set

We define first a Martin Lőf test, uniformly in the parameter  $k$ .

$$S_k = \bigcup_{n \geq 0} S_{k,n}$$

$$S_{k,0} = \emptyset$$

$S_{k,n+1}$  add to  $S_{k,n}$  the points that are **not** candidates to be normal, due to an initial segment of their expansions in some base.

$$S_{k,n} = \bigcup_{2 \leq b \leq B} \bigcup_{1 \leq \ell \leq L} \bigcup_{u \in \ell^*} \{w \in N^* : |\text{occ}(w, u) - N/b^\ell| > \varepsilon N\}$$

Using the Key Lemma,  $\mu(S_{k,n}) \leq 2L B^{3L-1} e^{-\varepsilon^2 N/3L} \leq \frac{1}{k} - \frac{1}{k+n}$ .

## Bonus Track: Turing's effective null set

We define first a Martin Lőf test, uniformly in the parameter  $k$ .

$$S_k = \bigcup_{n \geq 0} S_{k,n}$$

$$S_{k,0} = \emptyset$$

$S_{k,n+1}$  add to  $S_{k,n}$  the points that are **not** candidates to be normal, due to an initial segment of their expansions in some base.

$$S_{k,n} = \bigcup_{2 \leq b \leq B} \bigcup_{1 \leq \ell \leq L} \bigcup_{u \in \ell^*} \{w \in N^* : |\text{occ}(w, u) - N/b^\ell| > \varepsilon N\}$$

Using the Key Lemma,  $\mu(S_{k,n}) \leq 2L B^{3L-1} e^{-\varepsilon^2 N/3L} \leq \frac{1}{k} - \frac{1}{k+n}$ .

where

$N$ initial segment size	.....	linear in $n$	$N = k + n + 1$
$L$ block length	.....	sublogarithmic in $n$	$L = \sqrt{\log(k + n + 1)}/4$
$B$ base	.....	sublinear in $n$	$B = e^L$
$\varepsilon$ frequency discrepancy	....	goes to 0	$\varepsilon = B^{-L}$



## Bonus Track: Turing's effective null set

We define first a Martin Lőf test, uniformly in the parameter  $k$ .

$$S_k = \bigcup_{n \geq 0} S_{k,n}$$

$$S_{k,0} = \emptyset$$

$S_{k,n+1}$  add to  $S_{k,n}$  the points that are **not** candidates to be normal, due to an initial segment of their expansions in some base.

$$S_{k,n} = \bigcup_{2 \leq b \leq B} \bigcup_{1 \leq \ell \leq L} \bigcup_{u \in \ell^*} \{w \in N^* : |\text{occ}(w, u) - N/b^\ell| > \varepsilon N\}$$

Using the Key Lemma,  $\mu(S_{k,n}) \leq 2L B^{3L-1} e^{-\varepsilon^2 N/3L} \leq \frac{1}{k} - \frac{1}{k+n}$ .

where

$N$ initial segment size	.....	linear in $n$	$N = k + n + 1$
$L$ block length	.....	sublogarithmic in $n$	$L = \sqrt{\log(k+n+1)}/4$
$B$ base	.....	sublinear in $n$	$B = e^L$
$\varepsilon$ frequency discrepancy	....	goes to 0	$\varepsilon = B^{-L}$

Since  $S_k = \bigcup_{n \geq 0} S_{k,n}$ , then  $\mu(S_k) \leq \frac{1}{k}$ .

To obtain a Schnorr test adapt  $S_{k,n}$  to have exactly measure  $\frac{1}{k} - \frac{1}{k+n}$ .

# Normality and Incompressibility by Finite Automata

## Fixation

Fix a base  $b$ .

digits	=	digits in base $b$	=	$\mathcal{D} = \{0, \dots, b - 1\}$
blocks	=	finitely many digits	=	$b^*$
sequences	=	infinitely many digits	=	$b^\omega$

$$b^\omega \supset \{(\xi)_b : \xi \in [0, 1)\}$$

# Definition of normality

## Definition

The **block occurrences** of a block  $u$  inside a block  $w$  are

$$\text{blocc}(w, u) = |\{i : w[i|u|..(i+1)|u| - 1] = u\}|.$$

## Definition

$X \in b^\omega$  is **normal** if and only if for every block  $u$

$$\lim_{n \rightarrow \infty} \frac{\text{blocc}(X[1..n|u|], u)}{n} = b^{-|u|}.$$

$$X = (\xi)_b \quad \Rightarrow \quad \text{blocc}(X[1..n|u|], u) = \text{occ}((\xi)_{b|u|}[1..n], "u")$$

# Target acquired

Non-randomness can be characterized as compressibility:

$$\liminf_{n \rightarrow \infty} K_{\mathcal{U}}(X[1..n]) - n = -\infty \quad \Pi_2^0$$

What should we use to do the same for normality?

# Entropy

$$\lim_{n \rightarrow \infty} \frac{\text{blocc}(X[1..n|u|], u)}{n} = b^{-|u|}$$

frequency of  $u$  equal to  $b^{-|u|}$  looks familiar...

Shannon (1948):

- ▶ frequency of  $u$  other than  $b^{-|u|}$  implies non-maximum entropy
- ▶ non-maximum entropy implies compressibility

Huffman (1952):

- ▶ simple greedy implementation of Shannon's general idea
- ▶ such implementation can be coded into a Finite State Transducer

# Definition of transducers

## Definition

A **finite state transducer** is a tuple  $T = \langle Q, \delta, o, q_0 \rangle$ , where

- ▶  $Q$  is a finite set of states,
- ▶  $\delta : Q \times \mathcal{D} \rightarrow Q$  is the transition function,
- ▶  $o : Q \times \mathcal{D} \rightarrow b^*$  is the output function and
- ▶  $q_0 \in Q$  is the starting state.

$T$  processes sequences of digits in base  $b$ : if at state  $q$  digit  $d$  is processed,  $T$  moves to  $\delta(q, d)$  and outputs  $o(q, d)$ .

**transducer** = finite state transducer

$$\begin{array}{llll} \delta^*(q, \lambda) & = & q & \quad \quad \quad o^*(q, \lambda) & = & \lambda \\ \delta^*(q, du) & = & \delta^*(\delta(q, d), u) & \quad \quad \quad o^*(q, du) & = & o(q, d)o^*(\delta(q, d), u) \end{array}$$

$$T(u) = o^*(q_0, u) \quad \quad T(X) = \lim_{n \rightarrow \infty} T(X[1..n])$$

# Losses control

## Definition

A transducer  $T = \langle Q, \delta, o, q_0 \rangle$  is **lossless** if and only if  $u \mapsto \langle \delta^*(q_0, u), T(u) \rangle$  is injective.

## Definition

A transducer  $T = \langle Q, \delta, o, q_0 \rangle$  is **almost-everywhere-bounded-to-one** (aebt1) if and only if there is a measure one set  $\mathcal{X}$  such that  $X \mapsto T(X)$  is bounded to one in  $\mathcal{X}$ , i.e.,  $Y \mapsto |\{X \in \mathcal{X} : T(X) = Y\}|$  is bounded.

Lossless does not generalize well, but aebt1 does.



# Definition of compressibility

## Definition

An infinite sequence  $X$  is **compressible by finite automata** if and only if there is a bounded-to-one transducer  $T$  such that

$$\liminf_{n \rightarrow \infty} \frac{|T(X[1..n])|}{n} < 1$$

**compressible** = compressible by finite automata

## Theorem (Schnorr and Stimm)

*$X$  is compressible by  $T$  if and only if*

$$\liminf_{n \rightarrow \infty} |T(X[1..n])| - n = -\infty$$

# Non-normal in base $b$ vs non-random

## Theorem (Schnorr and Stimm)

$X$  is compressible by  $T$  if and only if

$$\liminf_{n \rightarrow \infty} |T(X[1..n])| - n = -\infty$$

$$\exists T \quad \liminf_{n \rightarrow \infty} |T(X[1..n])| - n = -\infty \quad \Sigma_3^0$$

$$\liminf_{n \rightarrow \infty} K_{\mathcal{U}}(X[1..n]) - n = -\infty \quad \Pi_2^0$$

## Theorem (Ki and Linton)

Normality in base  $b$  is  $\Pi_3^0$  complete.

# Not normal implies compressible

## Theorem (too many people)

*If  $X$  is not normal then it is compressible.*

Proof steps:

1. Fix the blocks and positions with non-maximum entropy
2. Codify the compression scheme for those blocks
3. Group blocks to minimize rounding problems
4. Profit

# Normal implies not compressible

## Theorem (too many people)

*If  $X$  is normal then it is not compressible.*

Proof steps:

1. Build a set of blocks with large contribution to the output
2. Show those are most of the blocks
3. Consider only the output of those blocks
4. Profit

# Who are those many people?

- ▶ Schnorr and Stimm  
abnormality  $\Leftrightarrow$  finite-state martingale success
- ▶ Dai, Lathrop, Lutz and Mayordomo  
compressibility  $\Leftrightarrow$  martingale success  
normality  $\Rightarrow$  no martingale success
- ▶ Bourke, Hitchcock and Vinodchandran  
non-normality  $\Rightarrow$  martingale success
- ▶ Becher and Heiber  
abnormality  $\Leftrightarrow$  compressibility (direct)
- ▶ Becher, Carton and Heiber  
generalized to bounded-to-one

# Meet in the middle

Normal incompressible by Finite-State Automata

⋮

?

⋮

Normal compressible by Turing Machines  
(Champernowne)

# Meet in the middle

Normal incompressible by Finite-State Automata

⋮

non-determinism   non-real-time   memory models

⋮

Normal compressible by Turing Machines  
(Champernowne)

## $k$ unary stacks automata

### Definition

A  $k$ -var transducer is a tuple  $T = \langle Q, \delta, \sigma_1, \dots, \sigma_k, o, q_0 \rangle$ , where

- ▶  $Q$  is a finite set of states,
- ▶  $\delta : Q \times \mathcal{D} \times \{0, 1\}^k \rightarrow Q$  is the transition function,
- ▶  $\sigma_i : Q \times \mathcal{D} \times \{0, 1\}^k \rightarrow \{-k, \dots, 0, \dots, k\}$  is the  $i$ -th variable function,
- ▶  $o : Q \times \mathcal{D} \times \{0, 1\}^k \rightarrow b^*$  is the output function and
- ▶  $q_0 \in Q$  is the starting state, with all empty stacks.

$T$  begins at state  $q_0$  with  $k$  integer variables with value 0. It then processes digits in base  $b$ : if at state  $q$  digit  $d$  is processed and  $(e_i)_{i \in 1, \dots, k}$  are bits representing if variable  $i$  is 0,  $T$  moves to state  $\delta(q, d, e_1, \dots, e_k)$ , outputs  $o(q, d, e_1, \dots, e_k)$  and adds  $\sigma_i(q, d, e_1, \dots, e_k)$  to variable  $i$ , capping to 0 if necessary.

lossless would require revisiting, but aebt1 works as is



# Normal implies not compressible (with $k$ unary stacks)

Theorem (Becher, Carton, Heiber)

*If  $X$  is normal then it is not compressible by  $k$ -var transducer.*

Proof steps:

1. Build a set of blocks with large contribution to the output
2. Show those are most of the blocks
3. Consider only the output of those blocks
4. Profit

# Non-deterministic automata

## Definition

A **non-deterministic transducer** is a tuple  $T = \langle \mathcal{Q}, \delta, \mathcal{Q}_a, q_0 \rangle$ , where

- ▶  $\mathcal{Q}$  is a finite set of states,
- ▶  $\delta : \mathcal{Q} \times \mathcal{D} \rightarrow \mathcal{P}(\mathcal{Q} \times b^*)$  is the non-deterministic transition and output function,
- ▶  $\mathcal{Q}_a \subseteq \mathcal{Q}$  is the set of accepting states and
- ▶  $q_0 \in \mathcal{Q}$  is the starting state.

$T$  processes sequences of digits in base  $b$ : if at state  $q$  digit  $d$  is processed,  $T$  may move to any state  $q'$  and output any block  $u'$  such that  $\langle q', u' \rangle \in \delta(q, d)$ . A computation is accepted if and only if it goes through an accepting state infinitely often.

lossless would require revisiting, but aebt1 works “as is”

## Definition

A non-deterministic transducer  $T = \langle \mathcal{Q}, \delta, q_0 \rangle$  is aebt1 if and only if there is a measure one set  $\mathcal{X}$  such that  $X \mapsto T(X)$  is bounded to one in  $\mathcal{X}$ , i.e.,  $Y \mapsto |\{X \in \mathcal{X} : T(X) \ni Y\}|$  is bounded.

# Normal implies not compressible (with non-deterministic)

Theorem (Becher, Carton, Heiber)

*If  $X$  is normal then it is not compressible by non-deterministic transducer.*

Proof steps:

1. Build a set of blocks with large contribution to the output
2. Show those are most of the blocks
3. Consider only the output of those blocks
4. Profit

# A small lemma

## Lemma (adapted from Schnorr and Stimm)

*The set of sequences that goes infinitely often through every state of a reachable strongly connected component of an automata has positive measure.*

Proof steps:

1. Fix a connected component and the path  $u$  that leads to it
2. Build accumulated paths  $u_{i,j}$  from each state to a given one
3. Consider the subset of  $[u]$  that contains  $u_{1,j}u_{2,j} \dots u_{n,j}$  an infinite number of times
4. Profit

# Non-deterministic stack automata

## Definition

A **non-deterministic  $k$ -ary stack transducer** is a tuple  $T = \langle Q, \delta, Q_a, q_0 \rangle$ , where

- ▶  $Q$  is a finite set of states,
- ▶  $\delta : Q \times \mathcal{D} \times \{0, \dots, k-1, \square\} \rightarrow \mathcal{P}(Q \times \{0, \dots, k-1\}^* \times b^*)$  is the non-deterministic transition and output function and
- ▶  $Q_a \subseteq Q$  is the set of accepting states and
- ▶  $q_0 \in Q$  is the starting state.

$T$  processes sequences of digits in base  $b$ : if at state  $q$  digit  $d$  is processed and  $c$  is on top of the stack,  $T$  pops  $c$  from the stack and may move to any state  $q'$ , push any  $k$ -sequence  $c'$  and output any block  $u'$  such that  $\langle q', c', u' \rangle \in \delta(q, d, c)$ . A computation is accepted if and only if it goes through an accepting state infinitely often.

lossless would require revisiting, but aebt1 works as is

# Normal does not imply not compressible (with non-deterministic and stack)

Theorem (Becher, Carton and Heiber on an idea of Boasson)

*There is a non-deterministic  $k$ -ary stack transducer that compresses a normal sequence.*

Proof steps:

1. Build a palindromic version of Champernowne
2. Show it is normal
3. Build a compressor of palindromes
4. Profit

## Bonus track: Selectors

### Definition

A **finite state selector** is a tuple  $T = \langle \mathcal{Q}, \delta, q_0, \mathcal{Q}_s \rangle$ , where

- ▶  $\mathcal{Q}$  is a finite set of states,
- ▶  $\delta : \mathcal{Q} \times \mathcal{D} \rightarrow \mathcal{Q}$  is the transition function,
- ▶  $\mathcal{Q}_s \subseteq \mathcal{Q}$  is the selecting set and
- ▶  $q_0 \in \mathcal{Q}$  is the starting state.

$T$  processes sequences of digits in base  $b$ : if at state  $q$  digit  $d$  is processed,  $T$  moves to  $\delta(q, d)$  and **outputs  $d$  if  $q \in \mathcal{Q}_s$  and nothing otherwise.**

**Theorem (Agafonov; Becher and Heiber)**

*Finite-state selectors preserve normality.*

## Other selection rules

Theorem (Agafonov; Becher and Heiber)

*Finite-state selectors preserve normality.*

Theorem (Merkle and Reimann)

*Finite-state 1-var selectors do not preserve normality.*

Theorem (Becher, Carton and Heiber)

*Non-deterministic selectors do not preserve normality.*

Selection to the left:

select  $X[i]$  based on  $X[1..i - 1]$  being in a certain language.

Selection to the right:

select  $X[i]$  based on  $X[i + 1..]$  being in a certain language.



## Other selection rules (cont.)

### Theorem (Merkle and Reimann)

*Selection to the left belonging to a linear language does not preserve normality.*

### Theorem (Becher, Carton and Heiber)

*Selection to the right suffix belonging to a set of infinite sequences recognizable by non-deterministic automata preserves normality.*

And finally, selection to the left and right simultaneously does not work:

### Theorem (Becher, Carton and Heiber)

*Selection of digits in between two zeros does not preserve normality.*

# Absolute Normality and Normality in Different Bases

# Today's topic: Constructions

1. An algorithm to compute absolutely normal numbers efficiently.
2. Constructions to exhibit different behavior relative to different bases.

# Absolutely normal numbers in just above quadratic time

## Theorem (Becher Heiber Slaman 2013)

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

Lutz and Mayordomo, and Figueira and Nies have other constructions, based on polynomial-time martingales.

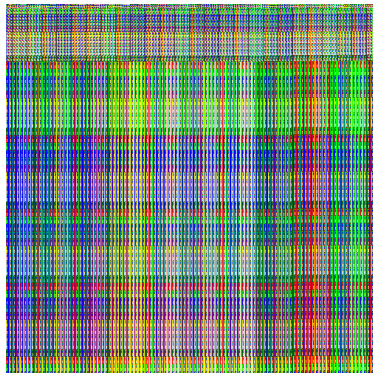
# The output of our algorithm in base 10

Programmed by Martin Epsztejn

0, 4031290542003809132371428380827059102765116777624189775110896366...



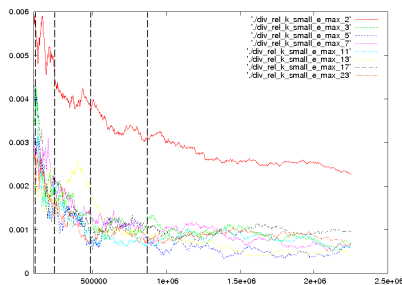
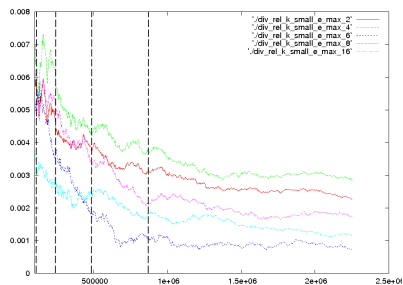
First 250000 digits output by the algorithm  
Plotted in 500x500 pixels, 10 colors



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

Algorithm with parameters  $t_i = (3 * \log(i)) + 3$ ;  $\varepsilon_i = 1/t_i$  Initial values  $t_1 = 3$ ;  $\varepsilon_1 = 1$ .  
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.

# Combinatorial discrepancy

Notation:  $\mathcal{L}(b, k)$  is the set of blocks in base  $b$  of length  $k$ .

## Definition

The *combinatorial discrepancy* of  $w \in \mathcal{L}(b, k)$  for blocks of length  $\ell$  is

$$D^c(\ell, w, b) = \max \left\{ \left| \frac{\text{occ}(w, u)}{k} - \frac{1}{b^\ell} \right| : u \in \mathcal{L}(b, \ell) \right\}.$$

For example, for  $b = 2$  and  $k = 4$

$w$	$D^c(1, w, b)$	$D^c(2, w, b)$
0000	$1 - 1/2 = 1/2$	$3/4 - 1/4 = 1/2$
0001	$3/4 - 1/2 = 1/4$	$1/4$
0010	$3/4 - 1/2 = 1/4$	$1/4$
0011	$0$	$1/4$
$\vdots$		

# Absolute normality

Recall, a real number  $\xi$  is *simply normal to base  $b$*  if each digit  $d$  in base  $b$

$$\lim_{n \rightarrow \infty} \text{occ}((\xi)_b[1..n], d)/n = 1/b.$$

## Theorem (Pillai 1940)

$\xi$  is absolutely normal if and only if it is simply normal to every base.

With the notation of combinatorial discrepancy, Pillai's Theorem reads:

A real number  $\xi$  is absolutely normal if and only if for every base  $b$ ,

$$\lim_{n \rightarrow \infty} D^c(1, (\xi)_b[1 \dots n], b) = 0.$$



# Almost all real numbers are normal

**Theorem (Borel 1909)**

*The set of absolutely normal numbers in the unit interval has Lebesgue measure one.*

# Almost all real numbers are normal

## Theorem (Borel 1909)

*The set of absolutely normal numbers in the unit interval has Lebesgue measure one.*

Effective version, based on Hardy and Wright's Key Lemma.

## Lemma

*Let  $\varepsilon$  and  $\delta$  be positive reals and  $b$  be a base. There is a  $k_0$  such that for every  $k \geq k_0$ ,*

$$\#\{w \in \mathcal{L}(b, k) : D^c(1, w, b) > \varepsilon\} < \delta b^k.$$

*Further, the value of  $k_0$  is uniformly computable, written  $K(\varepsilon, \delta, b)$ .*

# Notation

A rational number  $\xi$  in the unit interval is  $b$ -adic with precision  $n$  when

$$\xi = \sum_{j=1}^n d_j b^{-j} \text{ for digits } d_j \text{ in } \{0, \dots, b-1\}.$$

Thus,  $\xi$  is  $b$ -adic with precision  $n$  if  $\xi = a/b^n$ , for an integer  $a$  such that  $0 \leq a \leq b^n$ .

A  $b$ -adic semi-open interval is an interval of the form  $[a/b^n, (a+1)/b^n)$ , for  $0 \leq a < b^n$ .

We use  $\langle k; b \rangle$  to denote  $\lceil k/\log b \rceil$ .

## General construction of a computable real number

Consider a computable sequence  $(I)_{i \geq 1}$  of  $b$ -adic semi-open intervals  $I_i$  such that for all  $i \geq 1$ ,  $I_{i+1} \subset I_i$ ,  $\lim_{i \rightarrow \infty} \mu(I_i) = 0$  and  $\xi = \bigcap_{i \geq 1} I_i$ .

This yields a computation of  $\xi$  by specification of its infinite expansion in base  $b$ , from left to right. The real number  $\xi = \lim_{i \rightarrow \infty} \xi_i$  where  $\xi_{i+1}$  is obtained at step  $i + 1$  by **concatenating** the expansion of  $\xi_i$  with a new block of digits.

# Concatenation in a given base

We write  $*$  to denote concatenation of sequences.

## Lemma

Let  $x$  and  $u$  be blocks in base  $b$  and  $\varepsilon$  a real between 0 and 1.

1. If  $D^c(1, x, b) < \varepsilon$  and  $D^c(1, u, b) < \varepsilon$  then

$$D^c(1, x * u, b) < \varepsilon.$$

2. If  $D^c(1, x, b) < \varepsilon$  and  $|u|/|x| < \varepsilon$  then for every  $\ell$  such that  $1 \leq \ell \leq |u|$ ,

$$D^c(1, (x * u)[1, \dots, |x| + \ell], b) < 2\varepsilon.$$

## Concatenation does not translate well for base change

If  $\xi, \eta$  are  $b$ -adic rationals with precision  $n$  and  $\nu$  is a  $b$ -adic rational less than  $b^{-n}$  and with precision  $m$  then

$$(\xi + \nu)_b[n + 1 \dots (n + m)] = (\eta + \nu)_b[n + 1 \dots (n + m)].$$

However,

## Concatenation does not translate well for base change

If  $\xi, \eta$  are  $b$ -adic rationals with precision  $n$  and  $\nu$  is a  $b$ -adic rational less than  $b^{-n}$  and with precision  $m$  then

$$(\xi + \nu)_b[n + 1 \dots (n + m)] = (\eta + \nu)_b[n + 1 \dots (n + m)].$$

**However**, for a base  $a$  that is not a power of  $b$ , in general,

$$(\xi + \nu)_a[\langle n; a \rangle \dots \langle n + m; a \rangle] \neq (\eta + \nu)_a[\langle n; a \rangle \dots \langle n + m; a \rangle].$$

For instance, for  $b = 10$  and  $a = 3$ ,  $\xi = 25/100$ ,  $\eta = 50/100$ ,  $\nu = 17/10000$

---

$$(0.25)_3 = 0.020202020202\dots$$

$$(0.2517)_3 = 0.020210111012\dots$$

$$(0.50)_3 = 0.110111200011\dots$$

$$(0.5017)_3 = 0.111112201221\dots$$

---

## Definition of $t$ -sequences

### Lemma

*For any interval  $I$  and any base  $b$ , there is a  $b$ -adic subinterval  $I_b$  such that  $\mu(I_b) \geq \mu(I) / (2b)$ , where  $\mu(I)$  is the Lebesgue measure of  $I$ .*



# Definition of $t$ -sequences

## Lemma

For any interval  $I$  and any base  $b$ , there is a  $b$ -adic subinterval  $I_b$  such that  $\mu(I_b) \geq \mu(I)/(2b)$ , where  $\mu(I)$  is the Lebesgue measure of  $I$ .

## Definition

A  $t$ -sequence is a sequence of intervals,  $\vec{I} = (I_2, \dots, I_t)$ , such that

- ▶  $I_b$  is  $b$ -adic, for  $2 \leq b \leq t$
- ▶  $I_{b+1} \subseteq I_b$ , for  $2 \leq b < t$
- ▶  $\mu(I_{b+1}) \geq \mu(I_b)/2(b+1)$ , for  $2 \leq b < t$ .

# About $t$ -sequences

## Lemma

Let  $\vec{I} = (I_2, \dots, I_t)$  be a  $t$ -sequence. Then,  $\mu(I_t) \geq \mu(I_2) / (2^t t!)$ .

Notation: Let  $m(t) = 1 / (2^t t!)$ .

## Lemma (Lower bound for $t$ -sequences)

Let  $\vec{I}$  be a  $t$ -sequence. Let  $L$  be the largest dyadic subinterval of  $I_t$ . For any positive integer  $k$  consider the canonical partition of  $L$  in  $2^k$  subintervals  $L^{(h)}$ ,  $h = 0, \dots, 2^k - 1$ . For each such  $h$ , let  $\vec{J}^{(h)}$  be a  $(t+1)$ -sequence where  $J_{t+1}^{(h)} = L^{(h)}$ . Then,

$$\mu \left( \bigcup_{0 \leq h < 2^k} J_{t+1}^{(h)} \right) \geq m(t) m(t+1) \mu(I_2) / 4.$$

## $t$ -sequences good-for- $k$ -and- $\varepsilon$

### Definition

A  $t$ -sequence  $\vec{I}$  is *good-for- $k$ -and- $\varepsilon$*  if for each base  $b$  such that  $2 \leq b < t$ ,

$$D^c(1, u, b) \leq \varepsilon,$$

where  $I_b = [.w, .w + b^{-|w|})$  and  $u$  is the final block of  $w$  of length  $\langle k; b \rangle$ .

## $t$ -sequences good-for- $k$ -and- $\varepsilon$

### Definition

A  $t$ -sequence  $\vec{I}$  is *good-for- $k$ -and- $\varepsilon$*  if for each base  $b$  such that  $2 \leq b < t$ ,

$$D^c(1, u, b) \leq \varepsilon,$$

where  $I_b = [.w, .w + b^{-|w|})$  and  $u$  is the final block of  $w$  of length  $\langle k; b \rangle$ .

### Lemma (Upper bound for the not good)

Let  $\varepsilon$  and  $\delta$  be real numbers between 0 and 1,  $t$  be a base,  $\vec{I}$  be a  $t$ -sequence, and  $L$  be the largest dyadic subinterval of  $I_t$ . For  $k = K(\varepsilon, \delta, t) \lceil \log t \rceil$ , consider the canonical partition of  $L$  in  $2^k$  subintervals  $L^{(h)}$ ,  $h = 0, \dots, 2^k - 1$ . For each such  $h$ , let  $\vec{J}^{(h)}$  be a  $(t+1)$ -sequence where  $J_2^{(h)} = L^{(h)}$ . Then,

$$\mu \left( \bigcup_{0 \leq h < 2^k} J_{t+1}^{(h)} \text{ such that } \vec{J}^{(h)} \text{ is not good-for-}k\text{-and-}\varepsilon \right) < t_i \delta \mu(I_2).$$

# Algorithm

Let  $(\varepsilon_i)_{i \geq 1}$  computable non-increasing rationals that go to 0,  $\varepsilon_1 = 1$ .

Let  $(t_i)_{i \geq 1}$  computable non-decreasing unbounded sequence of bases,  $t_1 = 2$ .

The algorithm defines  $(\vec{I}_i)_{i \geq 1}$  of  $t_i$ -sequences  $\vec{I}_i = (I_{i,2}, \dots, I_{i,t_i})$ .

The constructed real  $\xi$  is the unique point in  $\bigcap_{i \geq 1} I_{i,2}$ .

# Algorithm

*Initial step.*  $I_{1,2} = [0, 1)$ .

*Recursion step  $i + 1$ .* We have a  $t_i$ -sequence  $\vec{I}_i$  from the previous stage.

1. Compute  $t_{i+1}$  and  $\varepsilon_{i+1}$ .  
Let  $\delta = 1/(2 t_i) m(t_i) m(t_{i+1})/4$  (controls the length of extension)  
Let  $k = K(\varepsilon_{i+1}, \delta, t_{i+1}) \lceil \log t_{i+1} \rceil$  (length of extension for base 2)
2. Let  $L$  be the largest dyadic subinterval of  $I_{i,t_i}$ .
3. Partition  $L$  in the  $2^k$  canonical subintervals  $L^{(h)}$ , for  $h = 0, \dots, 2^k - 1$ .
4. Find the leftmost  $t_{i+1}$ -sequence  $\vec{J}^{(h)}$  such that  $J_2^{(h)} = L^{(h)}$ , and  $J^{(h)}$  is good-for- $k$ -and- $\varepsilon_{i+1}$ , for  $h = 0, \dots, 2^k - 1$ .  
Let  $\vec{I}_{i+1}$  be such  $t_{i+1}$ -sequence.

## Correctness the algorithm

**The real  $\xi$  is well-defined.** At step  $i + 1$  the algorithm sets  $\delta = (1/2t_i)m(t_i) m(t_{i+1})/4$  and  $k = K(\varepsilon_{i+1}, \delta, t_{i+1}) \lceil \log t_{i+1} \rceil$ . By the lower bound for the  $t$ -sequences,

$$\mu \left( \bigcup_{0 \leq h < 2^k} J_{t_{i+1}}^{(h)} \right) \geq 2t_i \delta \mu(I_{i,2}).$$

By the upper bound for the not good  $t$ -sequences,

$$\mu \left( \bigcup_{0 \leq h < 2^k} J_{t_{i+1}}^{(h)} \text{ such that } \vec{J}^{(h)} \text{ is not good-for-}k\text{-and-}\varepsilon_{i+1} \right) < t_i \delta \mu(I_{i,2}).$$

So there is a  $t_{i+1}$ -sequence good-for- $k$ -and- $\varepsilon_{i+1}$ . The leftmost will be  $\vec{I}_{i+1}$ .

## Correctness the algorithm

**The real  $\xi$  is well-defined.** At step  $i + 1$  the algorithm sets  $\delta = (1/2t_i)m(t_i) m(t_{i+1})/4$  and  $k = K(\varepsilon_{i+1}, \delta, t_{i+1}) \lceil \log t_{i+1} \rceil$ . By the lower bound for the  $t$ -sequences,

$$\mu \left( \bigcup_{0 \leq h < 2^k} J_{t_{i+1}}^{(h)} \right) \geq 2t_i \delta \mu(I_{i,2}).$$

By the upper bound for the not good  $t$ -sequences,

$$\mu \left( \bigcup_{0 \leq h < 2^k} J_{t_{i+1}}^{(h)} \text{ such that } \vec{J}^{(h)} \text{ is not good-for-}k\text{-and-}\varepsilon_{i+1} \right) < t_i \delta \mu(I_{i,2}).$$

So there is a  $t_{i+1}$ -sequence good-for- $k$ -and- $\varepsilon_{i+1}$ . The leftmost will be  $\vec{I}_{i+1}$ .

**The real  $\xi$  is absolutely normal.** The construction iteratively adds short blocks of monotonically decreasing combinatorial discrepancy in each base. The bases go to infinity.



# The algorithm runs in polynomial time

At step  $i$  the algorithm searches over  $i$  different candidate sequences.  
The criteria for selection can be evaluated in polynomial time.  
Base change can be done in quadratic time.

# The algorithm runs in polynomial time

Assume  $(\varepsilon_i)_{i \geq 1}$  and  $(t_i)_{i \geq 1}$ .

*Recursion step  $i + 1$ .* We have a  $t_i$ -sequence  $\vec{I}_i$  from the previous stage.

1. Compute  $t_{i+1}$  and  $\varepsilon_{i+1}$ .

Let  $\delta = 1/(2 t_i) m(t_i) m(t_{i+1})$ .

Let  $k = K(\varepsilon_{i+1}, \delta, t_{i+1}) \lceil \log t_{i+1} \rceil$

**Incremental computation**

2. Let  $L$  be the largest dyadic subinterval of  $I_{i,t_i}$ .

**Base change**

3. Partition  $L$  in the  $2^k$  canonical subintervals  $L^{(h)}$ , for  $h = 0, \dots, 2^k - 1$ .

4. Find the leftmost  $t_{i+1}$ -sequence  $\vec{J}^{(h)}$  such that  $J_2^{(h)} = L^{(h)}$  and  $J^{(h)}$  is good-for- $k$ -and- $\varepsilon_{i+1}$ , for  $h = 0, \dots, 2^k - 1$ .

**At most  $(t_i \delta) 2^k$  ( $t_{i+1}$  base change + test good-for- $k$ -and- $\varepsilon_{i+1}$ )**

Let  $\vec{I}_{i+1}$  be such  $t_{i+1}$ -sequence.

Each test of good-for- $k$ -and- $\varepsilon_{i+1}$  runs in time linear in  $k$ . If  $t_i$  is sublinear in  $i$  and  $2^k$  is linear in  $i$  then the algorithm runs in polynomial time.

# Trading discrepancy for speed

Our algorithm achieves speed of computation at the cost of slowness of convergence to normality.

There are limits on the rate that discrepancy of a sequence of real numbers can converge to zero (Schmidt 1972) and there are absolutely normal numbers whose discrepancy are nearly optimal (M. L. Levin 1979).

## Question

*Is there an absolutely normal number computable in polynomial time whose discrepancy converges to zero at a nearly optimal rate?*

# A logical consequence of the method

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

1. *The set of indices for computable real numbers which are absolutely normal is  $\Pi_3^0$ -complete.*
2. *The set of real numbers that are absolutely normal is  $\Pi_3^0$ -complete.*

We give an algorithm uniformly on the  $\Pi_3^0$  sentence. If the  $\Pi_3^0$  sentence is true then real number constructed by the algorithm is absolutely normal. Else it is absolutely abnormal.

## Different bases

Now, we look at the issue of whether normality in one base is related to normality in another. We will see that except for one obvious condition, there is no dependence whatsoever.

# Multiplicative dependence

## Definition

For natural numbers  $s_1$  and  $s_2$  greater than 0, we say that  $s_1$  and  $s_2$  are *multiplicatively dependent* if each is a rational power of the other.

# Multiplicative dependence

## Definition

For natural numbers  $s_1$  and  $s_2$  greater than 0, we say that  $s_1$  and  $s_2$  are *multiplicatively dependent* if each is a rational power of the other.

## Theorem (Maxfield 1953)

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

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

# Multiplicative independence

Let  $M$  be the set of minimal representatives of the multiplicative dependence equivalence classes.

**Theorem (Schmidt 1961/62)**

*Let  $R$  be a subset of  $M$ . There is a real  $\xi$  such that  $\xi$  is normal to every base in  $R$  and not normal to any base in  $M \setminus R$ .*



# Multiplicative independence

Let  $M$  be the set of minimal representatives of the multiplicative dependence equivalence classes.

## Theorem (Schmidt 1961/62)

*Let  $R$  be a subset of  $M$ . There is a real  $\xi$  such that  $\xi$  is normal to every base in  $R$  and not normal to any base in  $M \setminus R$ .*

## Theorem (Becher and Slaman 2013)

*Let  $R$  be a  $\Pi_3^0$  subset of  $M$ . There is a real  $\xi$  such that  $\xi$  is normal to every base in  $R$  and not normal to any base in  $M \setminus R$ . Furthermore,  $\xi$  is uniformly computable in the  $\Pi_3^0$  formula which defines  $R$ .*

# Logical consequences

Confirming a conjecture of Ditzen (1994):

**Theorem (Becher and Slaman 2013)**

1. *The set of indices for computable real numbers which are normal some base is  $\Sigma_4^0$ -complete.*
2. *The set of real numbers that are normal to some base is  $\Sigma_4^0$ -complete.*

# Logical consequences

Confirming a conjecture of Ditzen (1994):

**Theorem (Becher and Slaman 2013)**

1. *The set of indices for computable real numbers which are normal some base is  $\Sigma_4^0$ -complete.*
2. *The set of real numbers that are normal to some base is  $\Sigma_4^0$ -complete.*

**Theorem (Becher and Slaman 2013)**

*For any  $\Pi_3^0$  formula  $\varphi$  there is a computable real  $\xi$  such that for any base  $r \in M$ ,  $\xi$  is normal to base  $r$  if and only if  $\varphi(\xi, r)$  is true.*

# Uniform distributions

characterizing normality

Let  $\{r^n \xi\}$  denote the fractional part of  $r^n \xi$ .

## Definition

A real number  $\xi$  is normal to base  $r$  iff the sequence  $(\{r^n \xi\} : 0 \leq n < \infty)$  is uniformly distributed in  $[0, 1]$ : for every  $0 \leq u < v \leq 1$ ,

$$\lim_{n \rightarrow \infty} \frac{\#\{n : 1 \leq n \leq N, u \leq \{r^n \xi\} < v\}}{N} = (v - u).$$

# Discrepancy

## Definition

Let  $N$  be a positive integer. Let  $\xi_1, \dots, \xi_N$  be real numbers in  $[0, 1]$ . The (metric) discrepancy of  $\xi_1, \dots, \xi_N$  is

$$D(\xi_1, \dots, \xi_N) = \sup_{0 \leq u < v \leq 1} \left| \frac{\#\{n : 1 \leq n \leq N, u \leq \xi_n < v\}}{N} - (v - u) \right|.$$

# Discrepancy

## Definition

Let  $N$  be a positive integer. Let  $\xi_1, \dots, \xi_N$  be real numbers in  $[0, 1]$ . The (metric) discrepancy of  $\xi_1, \dots, \xi_N$  is

$$D(\xi_1, \dots, \xi_N) = \sup_{0 \leq u < v \leq 1} \left| \frac{\#\{n : 1 \leq n \leq N, u \leq \xi_n < v\}}{N} - (v - u) \right|.$$

## Definition

Let  $r$  be a base. A real number  $\xi$  is normal to base  $r$  if and only if

$$\lim_{N \rightarrow \infty} D(\{r^j \xi : 0 \leq j \leq N\}) = 0.$$

# Convergence to normal

Are there dependencies between the discrepancy functions for different bases?

# Convergence to normal

Are there dependencies between the discrepancy functions for different bases?

**Theorem (Becher and Slaman 2013)**

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



# Simple normality

Sharpening Schmidt's theorem and addressing the issue raised by Brown, Moran and Pearce (1985):

**Theorem (Becher and Slaman 2013)**

*Let  $R$  be a subset of  $\mathbb{N}$  which is closed under multiplicative dependence. There is a real  $\xi$  such that  $\xi$  is normal to every base in  $R$  and not simply normal to any base in  $\mathbb{N} \setminus R$ . Furthermore, such a real can be obtained computably from  $R$ .*

# Proofs

We turn to the ingredients needed to establish these results, which will come from the related but diverse sources that have been brought to bear on normality.

# Proofs

We turn to the ingredients needed to establish these results, which will come from the related but diverse sources that have been brought to bear on normality.

To put the above sentence in context, we recall an exchange between characters in *The Matrix*, 1999:

# Proofs

We turn to the ingredients needed to establish these results, which will come from the related but diverse sources that have been brought to bear on normality.

To put the above sentence in context, we recall an exchange between characters in *The Matrix*, 1999:

*Neo: What does that mean?*

# Proofs

We turn to the ingredients needed to establish these results, which will come from the related but diverse sources that have been brought to bear on normality.

To put the above sentence in context, we recall an exchange between characters in *The Matrix*, 1999:

*Neo: What does that mean?*

*Cypher: It means, buckle your seat belt Dorothy, 'cause Kansas is going bye-bye.*

# Ingredients

Languages for Normality:

- ▶ Distributions of sequences modulo one
- ▶ Complex analysis and analytic number theory
- ▶ Combinatorics and counting occurrences of blocks of digits

# Ingredients

Languages for Normality:

- ▶ Distributions of sequences modulo one
- ▶ Complex analysis and analytic number theory
- ▶ Combinatorics and counting occurrences of blocks of digits

Computable constructions:

- ▶ Give finitary versions of asymptotic estimates provided by these tools.
- ▶ Use the finitary bounds in modules for constructions.
  - The typical module lowers discrepancy in bases  $r$  from a finite set  $R$  and increases discrepancy in a multiplicatively independent base  $s$ .

# Distributions of sequences

Effective version of  $D(\xi_1, \dots, \xi_N)$ :

## Definition

Let  $x_1, \dots, x_N$  be real numbers in  $[0, 1]$ . Let  $F$  be a family of semi-open intervals  $[a, b) \subset [0, 1]$ .

$$D(F, x_1, \dots, x_N) = \sup_{I \in F} \left| \frac{\#\{n : x_n \in I\}}{N} - \mu(I) \right|$$



# Distributions of sequences

Effective version of  $D(\xi_1, \dots, \xi_N)$ :

## Definition

Let  $x_1, \dots, x_N$  be real numbers in  $[0, 1]$ . Let  $F$  be a family of semi-open intervals  $[a, b) \subset [0, 1]$ .

$$D(F, x_1, \dots, x_N) = \sup_{I \in F} \left| \frac{\#\{n : x_n \in I\}}{N} - \mu(I) \right|$$

## Lemma

Suppose that  $\varepsilon$  is a real number strictly between 0 and 1. Let  $n = \lceil 3/\varepsilon \rceil$  and let  $F_\varepsilon$  be the family of semi-open intervals  $B_a = [a/n, (a+1)/n)$ , where  $0 \leq a < n$ . For any sequence  $\vec{\xi}$  and any  $N$ ,

$$D(F_\varepsilon, \vec{\xi}) < (\varepsilon/3)^2 \implies D(\vec{\xi}) < \varepsilon.$$

# The analytic perspective

Recall from Talk 1:

## Theorem (Weyl's Criterion)

A sequence  $(\xi_n : n \geq 1)$  of real numbers is uniformly distributed modulo one if and only if for every complex-valued, 1-periodic continuous function  $f$  we have

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{j=1}^N f(\xi_n) = \int_0^1 f(x) dx$$

that is, if and only if for every non-zero integer  $t$

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{j=1}^N e^{2\pi i t \xi_n} = 0.$$

# The analytic perspective

Effective version, uses LeVeque's Inequality:

## Lemma

*For any positive real  $\varepsilon$  there are a finite set of integers  $T$  and a positive real  $\delta$  such that for any  $\vec{\xi} = (\xi_1, \dots, \xi_N)$ , if for all  $t \in T$*

$$\frac{1}{N^2} \left| \sum_{j=1}^N e^{2\pi i t \xi_j} \right|^2 < \delta$$

*then  $D(\vec{\xi}) < \varepsilon$ . Furthermore, such  $T$  and  $\delta$  can be computed from  $\varepsilon$ .*

# Combinatorial discrepancy

## Definition

Fix a base  $s$ . The combinatorial discrepancy of  $w \in \mathcal{L}(s, N)$  (a base  $s$  word of length  $N$ ) for a block of size  $\ell$  is

$$D^c(\ell, w, s) = \max \left\{ \left| \frac{\text{occ}(w, u)}{N} - \frac{1}{s^\ell} \right| : u \in \mathcal{L}(s, \ell) \right\}.$$

# Combinatorial discrepancy

## Definition

Fix a base  $s$ . The combinatorial discrepancy of  $w \in \mathcal{L}(s, N)$  (a base  $s$  word of length  $N$ ) for a block of size  $\ell$  is

$$D^c(\ell, w, s) = \max \left\{ \left| \frac{\text{occ}(w, u)}{N} - \frac{1}{s^\ell} \right| : u \in \mathcal{L}(s, \ell) \right\}.$$

## Lemma

*For any  $\varepsilon > 0$ , if  $\ell$  is sufficiently large and  $N$  is sufficiently large relative to  $\ell$ , then for all  $w \in \mathcal{L}(s, N)$ ,*

$$D^c(\ell, w, s) < \varepsilon \implies D(\{s^j \eta_w\} : 0 \leq j < N) < \sqrt{18\varepsilon},$$

*where  $\eta_w$  is the rational  $w$  as the digits in its base  $s$  expansion and the sufficient conditions on  $\ell$  and  $N$  are computable from  $\varepsilon$ .*

# 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  $s - 2$  if  $s$  is even.

## Theorem (Schmidt 1960)

*Consider the fractal subset of  $[0, 1)$  represented by  $\mathcal{L}(\tilde{s}, \mathbb{N})$  in base  $s$  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(s) in its base  $s$  expansion and so is not be simply normal to base  $s$ .

## A discrepancy floor

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

Effective version:

### Lemma

*Let  $m$  be a positive integer and  $I$  an interval. Suppose that  $\vec{\xi}$  is a sequence of real numbers of length  $n \geq \lceil 2m/\mu(I) \rceil$  and that for all  $m \leq j \leq n$ ,  $\xi_j \notin I$ . Then,  $D(I, \vec{\xi}) \geq \mu(I)/2$ .*



# Conjoining finite random pieces

We have just observed that a random real from an  $\tilde{s}$ -fractal has prescribed normality and non-normality properties.

- ▶ Previously, we constructed absolutely normal numbers by conjoining longer and longer random finite strings.
- ▶ Here, we will do the same with random strings from  $\tilde{s}$ -fractals.

We will need translation invariant bounds on the lengths of the strings needed to capture lowered discrepancy.

# An analytic ceiling

Let  $\langle b; r \rangle$  denote  $\lceil b/\log r \rceil$  (normalizing a base  $r$  exponent). We systematize the sums in the effective Weyl Criterion:

# An analytic ceiling

Let  $\langle b; r \rangle$  denote  $\lceil b / \log r \rceil$  (normalizing a base  $r$  exponent). We systematize the sums in the effective Weyl Criterion:

## Definition

Let  $\xi$  be a real number,  $R$  be a finite set of bases,  $T$  be a finite set of non-zero integers,  $a$  be a non-negative integer, and  $u$  be a positive integer.

$$A(\xi, R, T, a, u) = \sum_{t \in T} \sum_{r \in R} \left| \sum_{j=\langle a; r \rangle+1}^{\langle a+u; r \rangle} e^{2\pi i t r^j \xi} \right|^2.$$

# An analytic ceiling

## Lemma (in the style of Schmidt)

Let  $R$  be a finite set of bases,  $T$  be a finite set of non-zero integers and  $s$  be a base multiplicatively independent to  $R$ . There is a function  $c(R, s)$  with positive values and a length  $u_0$  such that for all  $u \geq u_0$  the following holds. Suppose that  $\eta$  is  $s$ -adic with precision  $\langle a; s \rangle$ , and for  $v \in \mathcal{L}(\tilde{s}, N)$  let  $\eta_v$

denote the rational number  $\eta + s^{-\langle a; s \rangle} \sum_{j=1}^N v_j s^{-j}$ .

$$\#\{\eta_v : A(\eta_v, R, T, s, a, u) \leq u^{2-c(R,s)}\} \geq \frac{1}{2} \tilde{s}^{\langle a+u; s \rangle - \langle a; s \rangle}.$$

Further, the function  $c$  and the length  $u_0$  are uniformly computable from  $R$ ,  $T$  and  $s$ .

That is, for large precision in base  $s$ , more than half of the  $s$ -adic rationals in  $[\eta, \eta + s^{\langle a; s \rangle})$  which omit the last digit(s) in their base  $s$  expansions yield sub-quadratic values of  $A$ , which bounds their discrepancy in base  $r$  by the effective Weyl Criterion.

# A combinatorial ceiling

## Lemma

Let  $\varepsilon$  be a positive real, let  $s$  be a base and let  $\ell$  be positive integer. There is a  $k_0$  such that for every  $k \geq k_0$  there is an  $N_0$  such that for all  $N \geq N_0$ ,

$$\#\left\{w \in \mathcal{L}(\tilde{s}^k, N) : D^c(\ell, w, s) < \varepsilon\right\} > \frac{1}{2}\tilde{s}^{kN},$$

With the natural identification of  $w$  as a sequence in base  $s$ . Further, the values of  $k_0$  and  $N_0$  are uniformly computable.

Take  $k_0$  to be large enough so that almost all elements of  $s^{k_0}$  have combinatorial discrepancy less than  $\varepsilon$  for the appropriate block size. Then, take  $N$  to be large enough so that almost all length  $N_0$  sequences from  $\tilde{s}^k$  are within  $\varepsilon$  of simply normal.

# Constructions

We construct  $\xi$  by rational approximation.

- ▶ At stage  $m + 1$ , we are given  $\xi_m$  of the form  $\sum_{j=1}^{\langle b_m; s_m \rangle} v_j (s_m^{k_m})^{-j}$ , for some  $v \in \mathcal{L}(\langle b_m; s_m^{k_m} \rangle, s_m^{k_m})$ , with the intention that  $\xi \in [\xi_m, \xi_m + (s_m^{k_m})^{-\langle b_m; s_m^{k_m} \rangle})$ .
- ▶ We get  $\xi_{m+1} \in [\xi_m, \xi_m + (s_m^{k_m})^{-\langle b_m; s_m^{k_m} \rangle})$  in the  $s_{m+1}^{\tilde{k}_{m+1}}$ -fractal:
  - For all  $r$  in a finite set  $R_{m+1}$ , the discrepancy of  $(\{r^n \xi\} : \langle b_m; r \rangle < n \leq \langle b_{m+1}; r \rangle)$  is small, i.e. below the analytic ceiling appropriate for stage  $m + 1$ .
  - The discrepancy of  $(\{s_{m+1}^n \xi\} : \langle b_m; s_{m+1}^{k_{m+1}} \rangle < n \leq \langle b_{m+1}; s_{m+1}^{k_{m+1}} \rangle)$  is between the combinatorial ceiling and floor appropriate for  $s_{m+1}$  and  $k_{m+1}$ .

# The $\Pi_3^0$ theorem

**Theorem (Becher and Slaman 2013)**

*Let  $R$  be a  $\Pi_3^0$  subset of  $M$ . There is a real  $\xi$  such that  $\xi$  is normal to every base in  $R$  and not normal to any base in  $M \setminus R$ . Furthermore,  $\xi$  is uniformly computable in the  $\Pi_3^0$  formula which defines  $R$ .*

# The $\Pi_3^0$ theorem

**Theorem (Becher and Slaman 2013)**

*Let  $R$  be a  $\Pi_3^0$  subset of  $M$ . There is a real  $\xi$  such that  $\xi$  is normal to every base in  $R$  and not normal to any base in  $M \setminus R$ . Furthermore,  $\xi$  is uniformly computable in the  $\Pi_3^0$  formula which defines  $R$ .*

- ▶ Consider each base  $s$  infinitely often.
- ▶ For  $s$ , let  $n$  be the previous stage when we considered  $s$ , take  $x$  to be minimal such that there is a  $y$  less than  $\forall z < n \varphi(x, y, z)$  and  $\exists z < c \neg \varphi(x, y, z)$ .
  - Analytically lower the discrepancy ceiling for every base multiplicatively independent to  $s$  which has already appeared in the construction.
  - Combinatorially raise the discrepancy floor for  $s$  to level  $\varepsilon_x$  and keep the discrepancy ceiling below  $\varepsilon_{x-1}$ .



# Descriptive set theory

Theorem (Becher and Slaman 2013)

1. *The set of indices for computable real numbers which are normal some base is  $\Sigma_4^0$ -complete.*
2. *The set of real numbers that are normal to some base is  $\Sigma_4^0$ -complete.*

# Descriptive set theory

## Theorem (Becher and Slaman 2013)

1. *The set of indices for computable real numbers which are normal some base is  $\Sigma_4^0$ -complete.*
2. *The set of real numbers that are normal to some base is  $\Sigma_4^0$ -complete.*

- ▶ For (1), we exhibit a computable  $f$ , such that  $\exists x\varphi$  is true iff the computable real number named by  $f(\exists w\varphi)$  is normal to at least one base.
  - This follows from the  $\Pi_3^0$  theorem:  $f$  maps  $\exists w\varphi$  to the index for the computable  $\xi$  such that for all  $s_w \in M$ ,  $\xi$  is normal to base  $s_w$  if and only if  $\varphi(w)$  is true.
- ▶ (2) follows by relativization.

Similarly, the set of real numbers that are normal to infinitely many multiplicatively independent bases is  $\Pi_5^0$ -complete

# A fixed point

**Theorem (Becher and Slaman 2013)**

*For any  $\Pi_3^0$  formula  $\varphi$  there is a computable real  $\xi$  such that for any base  $r \in M$ ,  $\xi$  is normal to base  $r$  if and only if  $\varphi(\xi, r)$  is true.*

# A fixed point

## Theorem (Becher and Slaman 2013)

For any  $\Pi_3^0$  formula  $\varphi$  there is a computable real  $\xi$  such that for any base  $r \in M$ ,  $\xi$  is normal to base  $r$  if and only if  $\varphi(\xi, r)$  is true.

Let  $\varphi(X, x)$  be a  $\Pi_3^0$  formula.

- ▶ There is a computable  $f$  such that for every  $e$ , for all  $r \in M$ ,

$$\Psi_e \text{ is total and } \varphi(\Psi_e, r) \iff \Psi_{f(e)} \text{ is normal to base } r.$$

Furthermore, for every  $e$ ,  $\Psi_{f(e)}$  is total.

- ▶ By the Kleene Fixed Point Theorem, there is an  $e$  such that  $\Psi_e$  is equal to  $\Psi_{f(e)}$ . For this  $e$ , for all  $r \in M$ ,  
 $\varphi(\Psi_e, r)$  if and only if  $\Psi_e$  is normal to base  $r$ .

Then,  $\xi = \Psi_e$  satisfies the condition of the Theorem.

# Normality and Polynomial Time Martingales

# Base invariance of randomness notions

Algorithmic randomness notions are usually defined not for real numbers, but for their *digit representations* with respect to a fixed base.

A randomness notion  $\mathcal{R}$  is *base invariant* when

*if  $X$  and  $Y$  are infinite sequences over different alphabets that denote the same real, then  $X$  satisfies  $\mathcal{R}$  iff  $Y$  satisfies  $\mathcal{R}$ .*

# Proofs of base invariance

- ▶ Martin-Löf randomness is base invariant
  - Calude and Jürgensen (1994): using Martin-Löf tests
  - Staiger (1999): using prefix Kolmogorov Complexity
  - Hertling and Weihrauch (1998): topological approach
- ▶ Computable randomness is base invariant
  - Brattka, Miller and Nies (2011): using a correspondence between martingales and nondecreasing functions

# Outline

Notation and definitions



# Outline

Notation and definitions

Resource bounded versions of known results about martingales

# Outline

Notation and definitions

Resource bounded versions of known results about martingales

Base conversion

# Outline

Notation and definitions

Resource bounded versions of known results about martingales

Base conversion

Summary of Brattka, Miller, Nies 2011

# Outline

Notation and definitions

Resource bounded versions of known results about martingales

Base conversion

Summary of Brattka, Miller, Nies 2011

Polynomial time randomness is base invariant

# Outline

Notation and definitions

Resource bounded versions of known results about martingales

Base conversion

Summary of Brattka, Miller, Nies 2011

Polynomial time randomness is base invariant

Polynomial time randomness and normality

# Why polynomial time randomness?

- ▶ Applied side
  - Cryptography rely on pseudo-random generators
  - The quality of such pseudo-random sequences is measured by comparing them to benchmark “truly random” sequences
  - It suffices to take polynomial time random sequences.
  - The same for most practical applications.
- ▶ Mathematical side
  - an informal notion of randomness for sequences of bits has been used in an essential way in the recent work of Green and Tao showing that the set of primes has arbitrarily long arithmetic progressions
  - polynomial time randomness suffices

# Outline

Notation and definitions

Resource bounded versions of known results about martingales

Base conversion

Summary of Brattka, Miller, Nies 2011

Polynomial time randomness is base invariant

Polynomial time randomness and normality

# Notation

- ▶ A *rational in base  $r$*  is a rational number with finite representation in base  $r$ , i.e. a rational of the form  $z \cdot r^{-n}$ , for some  $z \in \mathbb{Z}$  and  $n \in \mathbb{N}$ .
  - $\mathbf{Rat}_r$  is the set of rationals in base  $r$
- ▶  $\Sigma_r = \{0, \dots, r - 1\}$
- ▶ We represent  $q \in \mathbf{Rat}_r$  with the pair  $\langle \sigma, \tau \rangle$ , where  $\sigma$  and  $\tau$  are strings in  $\Sigma_r^*$  representing the integer and fractional part of  $q$ , respectively. If  $p, q \in \mathbf{Rat}_r$  have both length  $n$  then
  - $\langle p, q \rangle \mapsto p + q \in \text{DTIME}(n)$
  - $\langle p, q \rangle \mapsto p \cdot q \in \text{DTIME}(n \cdot \log^2 n)$ .
- ▶ The function  $t$  will be a time bound such that  $t(n) \geq n$ .



# Martingales and randomness

## Definition

Let  $r \in \mathbb{N}$ ,  $r > 1$ .

- ▶ A *martingale in base  $r$*  is a function  $M : \Sigma_r^* \rightarrow \mathbb{R}^{\geq 0}$  such that

$$(\forall \sigma \in \Sigma_r^*) \quad r \cdot M(\sigma) = \sum_{b \in \Sigma_r} M(\sigma \hat{\ } b)$$

- ▶  $M$  is a  *$t(n)$ -martingale in base  $r$*  if  $M$  is  $\text{Rat}_r^{\geq 0}$ -valued and  $M \in \text{DTIME}(t(n))$ .
- ▶ We say that  $M$  *succeeds* on  $Z \in \Sigma_r^\infty$  iff  $\limsup_n M(Z \upharpoonright_n) = \infty$ .
- ▶ A sequence  $Z \in \Sigma_r^\infty$  is  *$t(n)$ -random in base  $r$*  if no  $t(n)$ -martingale in base  $r$  succeeds on  $Z$ .  $Z$  is *polynomial time random in base  $r$*  if  $Z$  is  $n^c$ -random for all  $c \geq 1$ .

# Computable approximation of a real function

## Definition

Let  $M : \Sigma_r^* \rightarrow \mathbb{R}^{\geq 0}$ . A computable function  $\widehat{M} : \Sigma_r^* \times \mathbb{N} \rightarrow \text{Rat}_r^{\geq 0}$  such that  $|\widehat{M}(\sigma, i) - M(\sigma)| \leq r^{-i}$  is called a *computable approximation* of  $M$ .

- ▶ The complexity of  $\widehat{M}$  on argument  $(\sigma, i)$  is measured in  $|\sigma| + i$ .
- ▶ A  $t(n)$ -computable approximation is a computable approximation in  $\text{DTIME}(t(n))$ .

# Outline

Notation and definitions

Resource bounded versions of known results about martingales

Base conversion

Summary of Brattka, Miller, Nies 2011

Polynomial time randomness is base invariant

Polynomial time randomness and normality

# Real-valued to rational-valued martingales

## Lemma

*If  $M$  is a martingale in base  $r$  with a  $t(n)$ -computable approximation then there is an  $n \cdot t(n)$ -martingale  $N$  in base  $r$  such that  $N \geq M$ .*

## Savings property

If  $M$  is a martingale in base  $r$  then

$$M(\sigma) \leq M(\emptyset) \cdot r^{|\sigma|}.$$

We say that a martingale  $M$  in base  $r$  has the *savings property* if there is  $c > 0$  such that for all  $\tau, \sigma \in \Sigma_r^*$ ,

$$\tau \succeq \sigma \Rightarrow M(\sigma) - M(\tau) \leq c.$$

## Savings property

If  $M$  is a martingale in base  $r$  then

$$M(\sigma) \leq M(\emptyset) \cdot r^{|\sigma|}.$$

We say that a martingale  $M$  in base  $r$  has the *savings property* if there is  $c > 0$  such that for all  $\tau, \sigma \in \Sigma_r^*$ ,

$$\tau \succeq \sigma \Rightarrow M(\sigma) - M(\tau) \leq c.$$

### Proposition

*Suppose  $M$  is a martingale in base  $r$  with the savings property via  $c$ . Then*

$$(\forall \sigma \in \Sigma_r^*) M(\sigma) \leq (r - 1) \cdot c \cdot |\sigma| + M(\emptyset).$$

## Savings property

If  $M$  is a martingale in base  $r$  then

$$M(\sigma) \leq M(\emptyset) \cdot r^{|\sigma|}.$$

We say that a martingale  $M$  in base  $r$  has the *savings property* if there is  $c > 0$  such that for all  $\tau, \sigma \in \Sigma_r^*$ ,

$$\tau \succeq \sigma \Rightarrow M(\sigma) - M(\tau) \leq c.$$

### Proposition

Suppose  $M$  is a martingale in base  $r$  with the savings property via  $c$ . Then

$$(\forall \sigma \in \Sigma_r^*) M(\sigma) \leq (r - 1) \cdot c \cdot |\sigma| + M(\emptyset).$$

### Lemma (Time bounded savings property)

For each  $t(n)$ -martingale  $L$  in base  $r$  there is an  $n \cdot t(n)$ -martingale  $M$  in base  $r$  such that

- ▶  $M$  has the savings property and
- ▶  $M$  succeeds on all the sequences that  $L$  succeeds on.

## Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

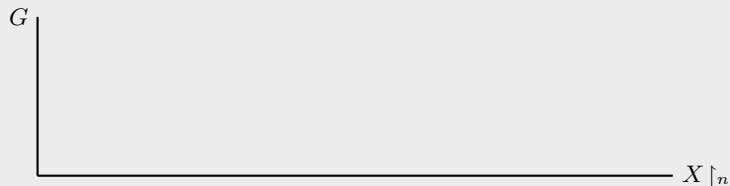
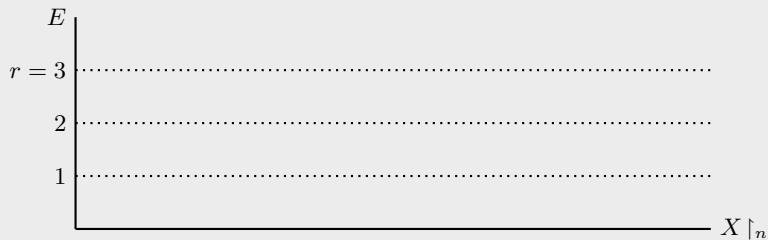


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example



# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

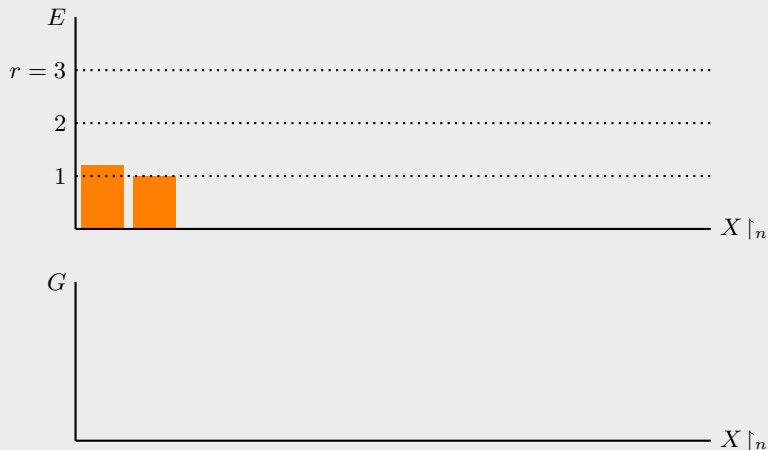


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

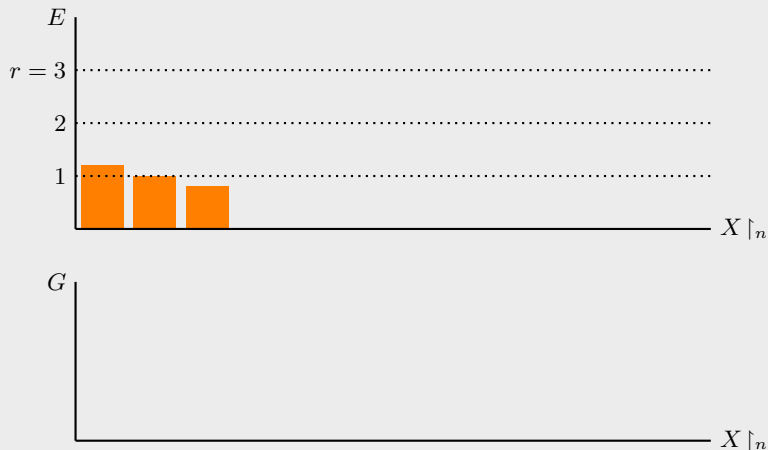


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

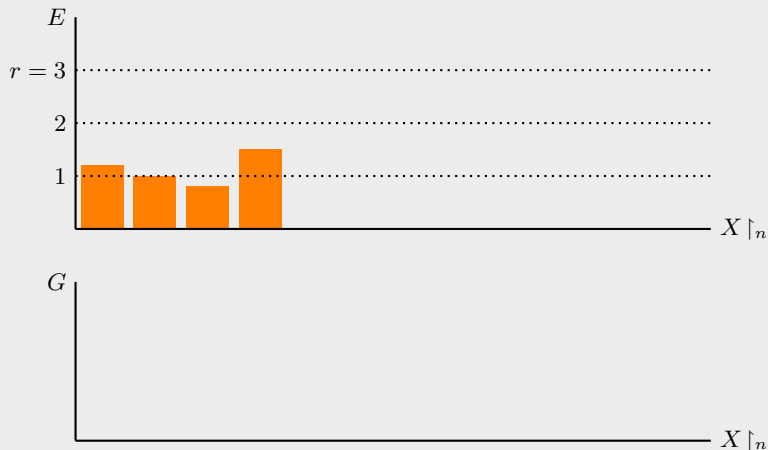


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

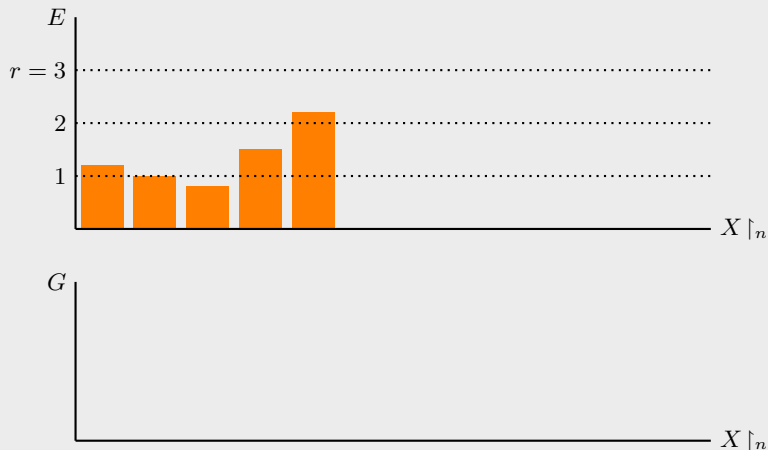


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

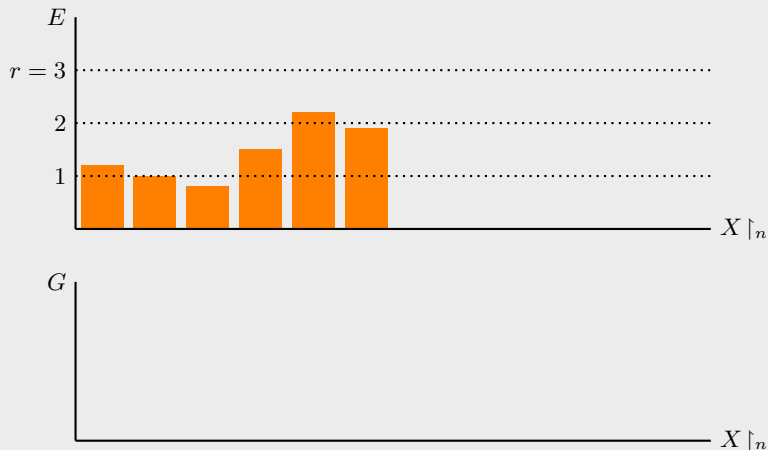


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

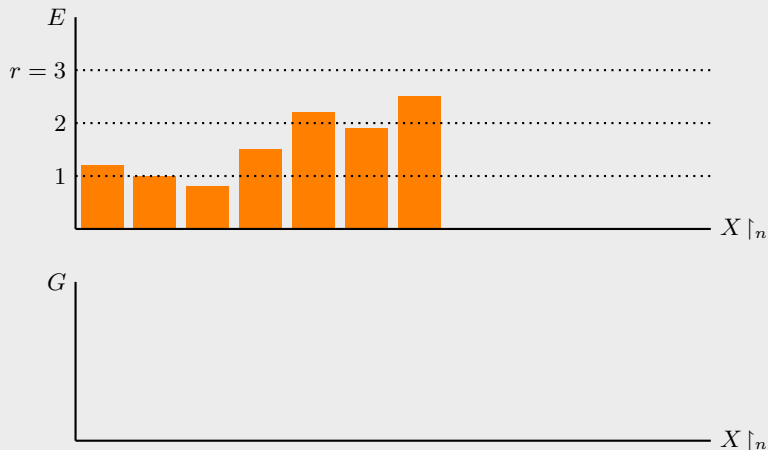


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example



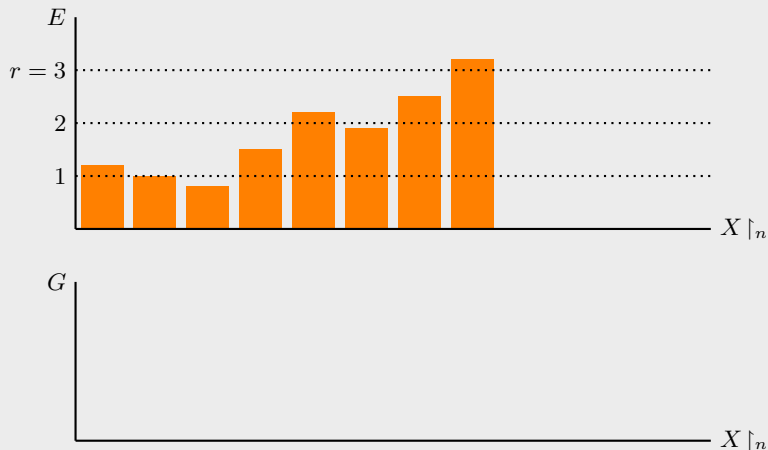


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

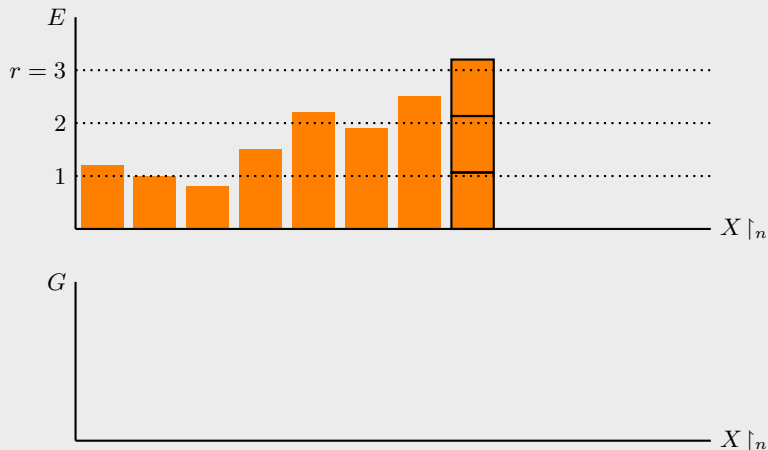


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

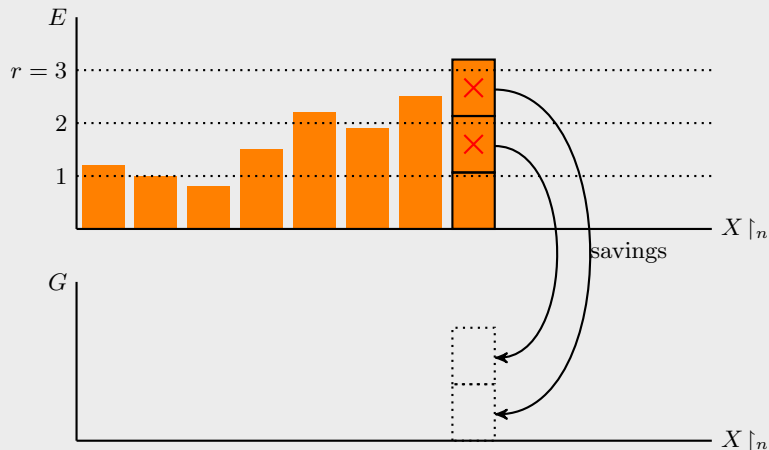


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

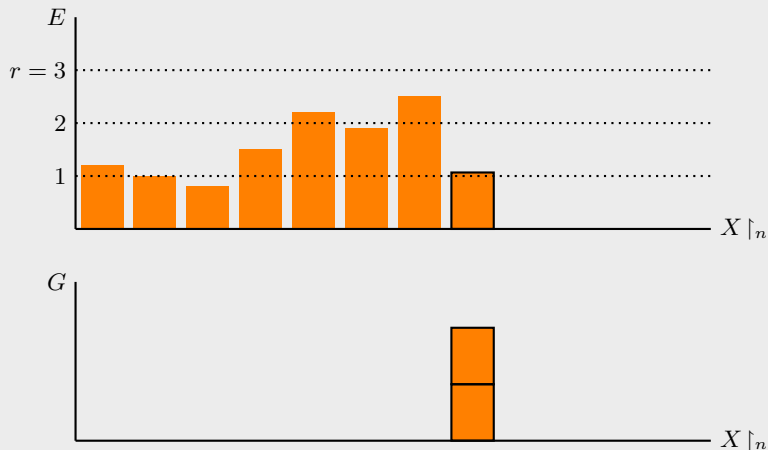


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

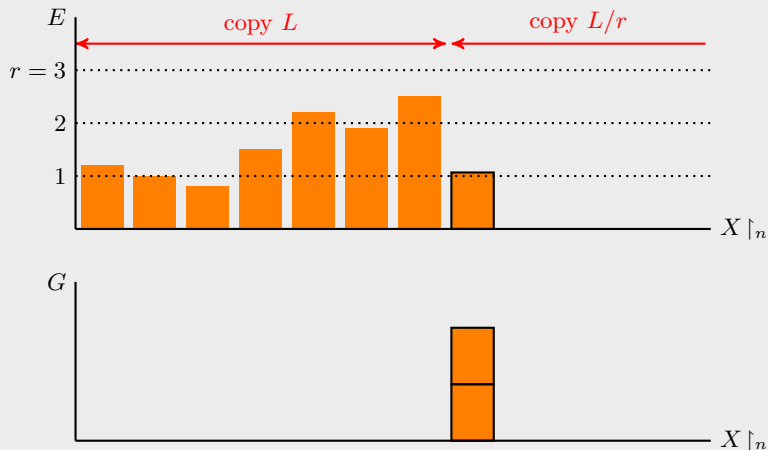


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

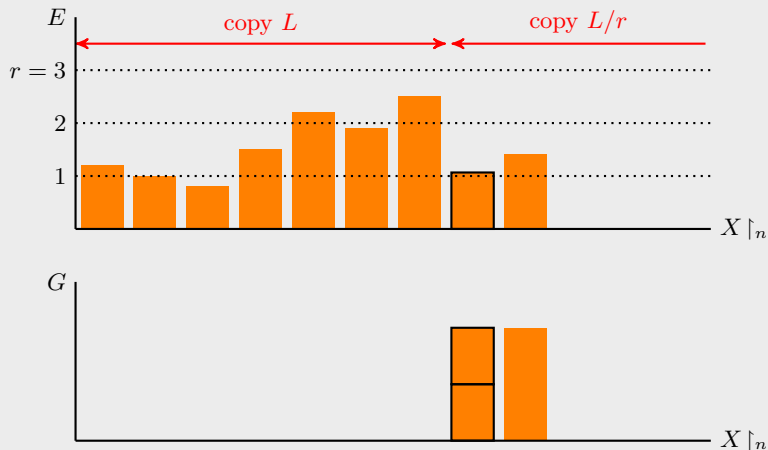


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

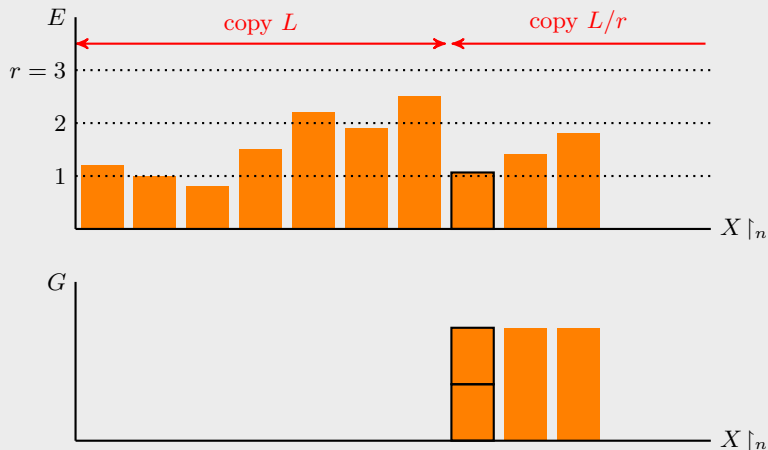


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example

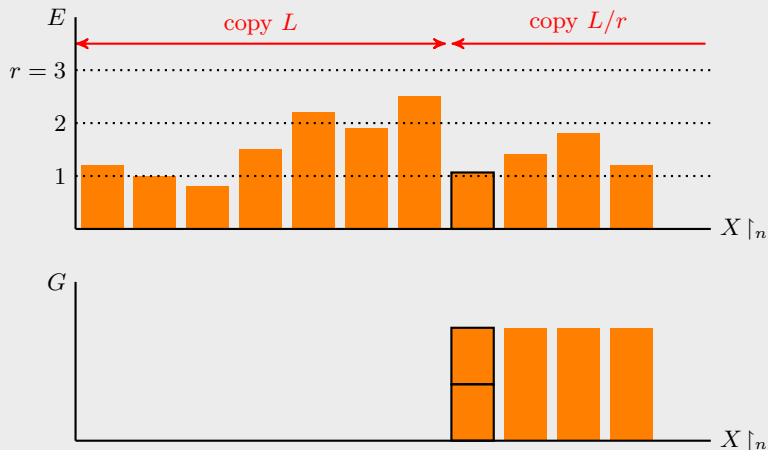


# Savings property

Given a  $t(n)$ -martingale  $L$  in base  $r$ , let  $M = G + E$ , where

- ▶  $G(\sigma)$  is the balance of the savings account at  $\sigma$
- ▶  $E(\sigma)$  is the balance of the checking account at  $\sigma$

## Example





## Savings property

Wlog, assume  $L(\emptyset) \leq 1$ .

Let  $E(\emptyset) = L(\emptyset)$ ,  $G(\emptyset) = 0$ . For each  $b \in \Sigma_r$  and  $\sigma \in \Sigma_r^*$ , let

$$\begin{aligned}\alpha_b(\sigma) &= L(\sigma \hat{\ } b) \cdot E(\sigma) / L(\sigma) \\ E(\sigma \hat{\ } b) &= \begin{cases} \alpha_b(\sigma) / r & \text{if } \alpha_b(\sigma) > r \\ \alpha_b(\sigma) & \text{otherwise} \end{cases} \\ G(\sigma \hat{\ } b) &= \begin{cases} G(\sigma) + \alpha_b(\sigma) \cdot (r - 1) / r & \text{if } \alpha_b(\sigma) > r \\ G(\sigma) & \text{otherwise} \end{cases}\end{aligned}$$

Define  $M = E + G$ .

## Savings property

Wlog, assume  $L(\emptyset) \leq 1$ .

Let  $E(\emptyset) = L(\emptyset)$ ,  $G(\emptyset) = 0$ . For each  $b \in \Sigma_r$  and  $\sigma \in \Sigma_r^*$ , let

$$\begin{aligned}\alpha_b(\sigma) &= L(\sigma \hat{b}) \cdot E(\sigma) / L(\sigma) \\ E(\sigma \hat{b}) &= \begin{cases} \alpha_b(\sigma) / r & \text{if } \alpha_b(\sigma) > r \\ \alpha_b(\sigma) & \text{otherwise} \end{cases} \\ G(\sigma \hat{b}) &= \begin{cases} G(\sigma) + \alpha_b(\sigma) \cdot (r - 1) / r & \text{if } \alpha_b(\sigma) > r \\ G(\sigma) & \text{otherwise} \end{cases}\end{aligned}$$

Define  $M = E + G$ .

- ▶  $E$  and  $G$  are  $\text{Rat}_r^{\geq 0}$ -valued, so  $M$  is  $\text{Rat}_r^{\geq 0}$ -valued

## Savings property

Wlog, assume  $L(\emptyset) \leq 1$ .

Let  $E(\emptyset) = L(\emptyset)$ ,  $G(\emptyset) = 0$ . For each  $b \in \Sigma_r$  and  $\sigma \in \Sigma_r^*$ , let

$$\begin{aligned}\alpha_b(\sigma) &= L(\sigma \hat{b}) \cdot E(\sigma) / L(\sigma) \\ E(\sigma \hat{b}) &= \begin{cases} \alpha_b(\sigma) / r & \text{if } \alpha_b(\sigma) > r \\ \alpha_b(\sigma) & \text{otherwise} \end{cases} \\ G(\sigma \hat{b}) &= \begin{cases} G(\sigma) + \alpha_b(\sigma) \cdot (r - 1) / r & \text{if } \alpha_b(\sigma) > r \\ G(\sigma) & \text{otherwise} \end{cases}\end{aligned}$$

Define  $M = E + G$ .

- ▶  $E$  and  $G$  are  $\text{Rat}_r^{\geq 0}$ -valued, so  $M$  is  $\text{Rat}_r^{\geq 0}$ -valued
- ▶  $M(\sigma \hat{b}) = E(\sigma \hat{b}) + G(\sigma \hat{b}) = \alpha_b(\sigma) + G(\sigma)$

## Savings property

Wlog, assume  $L(\emptyset) \leq 1$ .

Let  $E(\emptyset) = L(\emptyset)$ ,  $G(\emptyset) = 0$ . For each  $b \in \Sigma_r$  and  $\sigma \in \Sigma_r^*$ , let

$$\begin{aligned}\alpha_b(\sigma) &= L(\sigma \hat{b}) \cdot E(\sigma) / L(\sigma) \\ E(\sigma \hat{b}) &= \begin{cases} \alpha_b(\sigma) / r & \text{if } \alpha_b(\sigma) > r \\ \alpha_b(\sigma) & \text{otherwise} \end{cases} \\ G(\sigma \hat{b}) &= \begin{cases} G(\sigma) + \alpha_b(\sigma) \cdot (r - 1) / r & \text{if } \alpha_b(\sigma) > r \\ G(\sigma) & \text{otherwise} \end{cases}\end{aligned}$$

Define  $M = E + G$ .

- ▶  $E$  and  $G$  are  $\text{Rat}_r^{\geq 0}$ -valued, so  $M$  is  $\text{Rat}_r^{\geq 0}$ -valued
- ▶  $M(\sigma \hat{b}) = E(\sigma \hat{b}) + G(\sigma \hat{b}) = \alpha_b(\sigma) + G(\sigma)$
- ▶  $L$  is a martingale  $\Rightarrow M$  is a martingale

## Savings property

Wlog, assume  $L(\emptyset) \leq 1$ .

Let  $E(\emptyset) = L(\emptyset)$ ,  $G(\emptyset) = 0$ . For each  $b \in \Sigma_r$  and  $\sigma \in \Sigma_r^*$ , let

$$\begin{aligned}\alpha_b(\sigma) &= L(\sigma \hat{b}) \cdot E(\sigma) / L(\sigma) \\ E(\sigma \hat{b}) &= \begin{cases} \alpha_b(\sigma) / r & \text{if } \alpha_b(\sigma) > r \\ \alpha_b(\sigma) & \text{otherwise} \end{cases} \\ G(\sigma \hat{b}) &= \begin{cases} G(\sigma) + \alpha_b(\sigma) \cdot (r - 1) / r & \text{if } \alpha_b(\sigma) > r \\ G(\sigma) & \text{otherwise} \end{cases}\end{aligned}$$

Define  $M = E + G$ .

- ▶  $E$  and  $G$  are  $\text{Rat}_r^{\geq 0}$ -valued, so  $M$  is  $\text{Rat}_r^{\geq 0}$ -valued
- ▶  $M(\sigma \hat{b}) = E(\sigma \hat{b}) + G(\sigma \hat{b}) = \alpha_b(\sigma) + G(\sigma)$
- ▶  $L$  is a martingale  $\Rightarrow M$  is a martingale
- ▶  $\tau \succeq \sigma \Rightarrow G(\tau) \geq G(\sigma)$

# Savings property

Wlog, assume  $L(\emptyset) \leq 1$ .

Let  $E(\emptyset) = L(\emptyset)$ ,  $G(\emptyset) = 0$ . For each  $b \in \Sigma_r$  and  $\sigma \in \Sigma_r^*$ , let

$$\begin{aligned}\alpha_b(\sigma) &= L(\sigma \hat{\ } b) \cdot E(\sigma) / L(\sigma) \\ E(\sigma \hat{\ } b) &= \begin{cases} \alpha_b(\sigma) / r & \text{if } \alpha_b(\sigma) > r \\ \alpha_b(\sigma) & \text{otherwise} \end{cases} \\ G(\sigma \hat{\ } b) &= \begin{cases} G(\sigma) + \alpha_b(\sigma) \cdot (r - 1) / r & \text{if } \alpha_b(\sigma) > r \\ G(\sigma) & \text{otherwise} \end{cases}\end{aligned}$$

Define  $M = E + G$ .

- ▶  $E$  and  $G$  are  $\text{Rat}_r^{\geq 0}$ -valued, so  $M$  is  $\text{Rat}_r^{\geq 0}$ -valued
- ▶  $M(\sigma \hat{\ } b) = E(\sigma \hat{\ } b) + G(\sigma \hat{\ } b) = \alpha_b(\sigma) + G(\sigma)$
- ▶  $L$  is a martingale  $\Rightarrow M$  is a martingale
- ▶  $\tau \succeq \sigma \Rightarrow G(\tau) \geq G(\sigma)$
- ▶  $\tau \succeq \sigma \Rightarrow M(\sigma) - M(\tau) \leq E(\sigma) - E(\tau) \leq E(\sigma) \leq r$

## Savings property

Wlog, assume  $L(\emptyset) \leq 1$ .

Let  $E(\emptyset) = L(\emptyset)$ ,  $G(\emptyset) = 0$ . For each  $b \in \Sigma_r$  and  $\sigma \in \Sigma_r^*$ , let

$$\begin{aligned}\alpha_b(\sigma) &= L(\sigma \hat{\ } b) \cdot E(\sigma) / L(\sigma) \\ E(\sigma \hat{\ } b) &= \begin{cases} \alpha_b(\sigma) / r & \text{if } \alpha_b(\sigma) > r \\ \alpha_b(\sigma) & \text{otherwise} \end{cases} \\ G(\sigma \hat{\ } b) &= \begin{cases} G(\sigma) + \alpha_b(\sigma) \cdot (r - 1) / r & \text{if } \alpha_b(\sigma) > r \\ G(\sigma) & \text{otherwise} \end{cases}\end{aligned}$$

Define  $M = E + G$ .

- ▶  $E$  and  $G$  are  $\text{Rat}_r^{\geq 0}$ -valued, so  $M$  is  $\text{Rat}_r^{\geq 0}$ -valued
- ▶  $M(\sigma \hat{\ } b) = E(\sigma \hat{\ } b) + G(\sigma \hat{\ } b) = \alpha_b(\sigma) + G(\sigma)$
- ▶  $L$  is a martingale  $\Rightarrow M$  is a martingale
- ▶  $\tau \succeq \sigma \Rightarrow G(\tau) \geq G(\sigma)$
- ▶  $\tau \succeq \sigma \Rightarrow M(\sigma) - M(\tau) \leq E(\sigma) - E(\tau) \leq E(\sigma) \leq r$
- ▶  $\limsup_n L(X \upharpoonright_n) = \infty \Rightarrow \lim_n G(X \upharpoonright_n) = \infty$

## Savings property

For  $\sigma \in \Sigma_r^n$ , let  $I_\sigma$  be the maximal sequence

$$-1 = i_0 < i_1 < \cdots < i_{k_\sigma} < i_{k_\sigma+1} = n$$

such that

$$\begin{aligned} & (\forall p = 1, \dots, k_\sigma) L(\sigma \upharpoonright_{i_{p+1}}) > r^p \\ & (\forall p \in \{0, \dots, k_\sigma\}) (\forall m \in \{i_p + 2, \dots, i_{p+1}\}) L(\sigma \upharpoonright_m) \leq r^p. \end{aligned}$$



# Savings property

For  $\sigma \in \Sigma_r^n$ , let  $I_\sigma$  be the maximal sequence

$$-1 = i_0 < i_1 < \cdots < i_{k_\sigma} < i_{k_\sigma+1} = n$$

such that

$$\begin{aligned} &(\forall p = 1, \dots, k_\sigma) L(\sigma \upharpoonright_{i_{p+1}}) > r^p \\ &(\forall p \in \{0, \dots, k_\sigma\})(\forall m \in \{i_p + 2, \dots, i_{p+1}\}) L(\sigma \upharpoonright_m) \leq r^p. \end{aligned}$$

**Fact**

$$E(\sigma) = L(\sigma)/r^{k_\sigma} \text{ and } G(\sigma) = (r - 1) \cdot \sum_{p=1}^{k_\sigma} L(\sigma \upharpoonright_{i_{p+1}})/r^p.$$

# Savings property

For  $\sigma \in \Sigma_r^n$ , let  $I_\sigma$  be the maximal sequence

$$-1 = i_0 < i_1 < \dots < i_{k_\sigma} < i_{k_\sigma+1} = n$$

such that

$$\begin{aligned} & (\forall p = 1, \dots, k_\sigma) L(\sigma \upharpoonright_{i_{p+1}}) > r^p \\ & (\forall p \in \{0, \dots, k_\sigma\}) (\forall m \in \{i_p + 2, \dots, i_{p+1}\}) L(\sigma \upharpoonright_m) \leq r^p. \end{aligned}$$

## Fact

$$E(\sigma) = L(\sigma)/r^{k_\sigma} \text{ and } G(\sigma) = (r-1) \cdot \sum_{p=1}^{k_\sigma} L(\sigma \upharpoonright_{i_{p+1}})/r^p.$$

- ▶  $I_\sigma \in \text{DTIME}(n \cdot t(n))$
- ▶  $E(\sigma), G(\sigma) \in \text{DTIME}(n \cdot t(n))$
- ▶  $M$  is an  $n \cdot t(n)$ -martingale in base  $r$ .

# Outline

Notation and definitions

Resource bounded versions of known results about martingales

**Base conversion**

Summary of Brattka, Miller, Nies 2011

Polynomial time randomness is base invariant

Polynomial time randomness and normality

## More notation

- ▶ If  $\sigma \in \Sigma_r^*$  then  $\langle 0.\sigma \rangle_r$  represents the rational in  $[0, 1]$  whose representation in base  $r$  is  $0.\sigma$ , i.e.

$$\langle 0.\sigma \rangle_r = \sum_{i=0}^{|\sigma|-1} \sigma(i) \cdot r^{-i-1}.$$

- ▶ If  $Z \in \Sigma_r^\infty$ , then  $\langle 0.Z \rangle_r$  represents the real in  $[0, 1]$  whose expansion in base  $r$  is  $Z$ , i.e.

$$\langle 0.Z \rangle_r = \sum_{i \in \mathbb{N}} Z(i) \cdot r^{-i-1}.$$

# Base conversion

We want a functional  $\Gamma : \Sigma_r^\infty \times \mathbb{N} \rightarrow \Sigma_s$  which converts from base  $r$  to base  $s$ :

for all  $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

# Base conversion

We want a functional  $\Gamma : \Sigma_r^\infty \times \mathbb{N} \rightarrow \Sigma_s$  which converts from base  $r$  to base  $s$ :

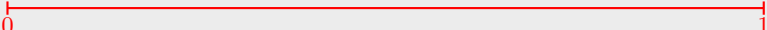
for all  $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

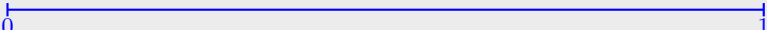
$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

## Example

$X = \dots$

$Y = \dots$

$r = 3$     0  1

$r = 2$     0  1

# Base conversion

We want a functional  $\Gamma : \Sigma_r^\infty \times \mathbb{N} \rightarrow \Sigma_s$  which converts from base  $r$  to base  $s$ :

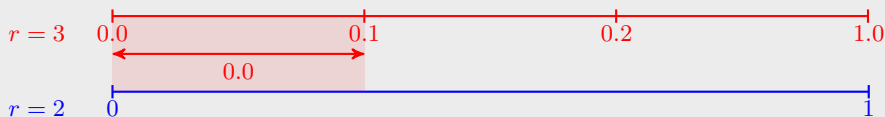
for all  $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

## Example

$X = 0\dots$

$Y = \dots$



# Base conversion

We want a functional  $\Gamma : \Sigma_r^\infty \times \mathbb{N} \rightarrow \Sigma_s$  which converts from base  $r$  to base  $s$ :

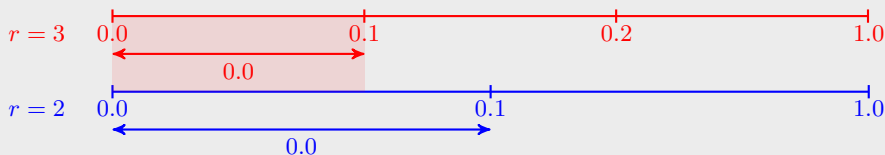
for all  $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

## Example

$X = 0\dots$

$Y = 0\dots$





# Base conversion

We want a functional  $\Gamma : \Sigma_r^\infty \times \mathbb{N} \rightarrow \Sigma_s$  which converts from base  $r$  to base  $s$ :

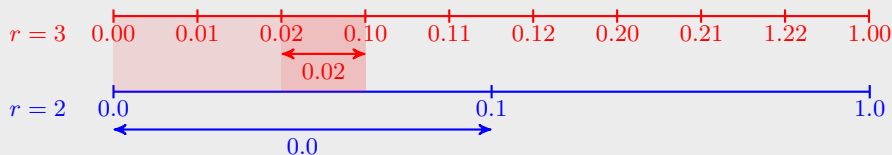
for all  $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

## Example

$X = 02\dots$

$Y = 0\dots$



# Base conversion

We want a functional  $\Gamma : \Sigma_r^\infty \times \mathbb{N} \rightarrow \Sigma_s$  which converts from base  $r$  to base  $s$ :

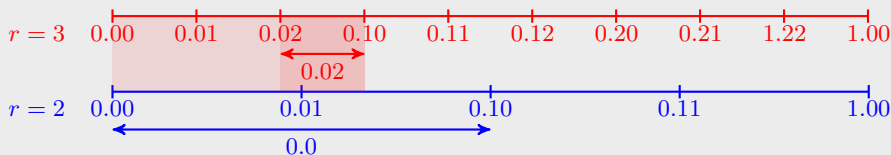
for all  $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

## Example

$X = 02\dots$

$Y = 0\dots$



# Base conversion

We want a functional  $\Gamma : \Sigma_r^\infty \times \mathbb{N} \rightarrow \Sigma_s$  which converts from base  $r$  to base  $s$ :

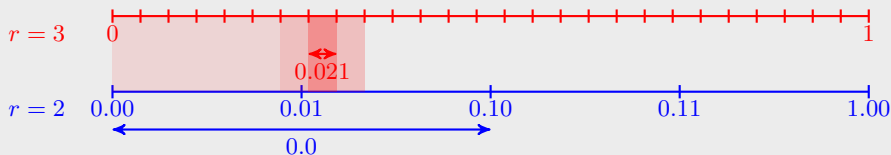
for all  $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

## Example

$X = 021\dots$

$Y = 0\dots$



# Base conversion

We want a functional  $\Gamma : \Sigma_r^\infty \times \mathbb{N} \rightarrow \Sigma_s$  which converts from base  $r$  to base  $s$ :

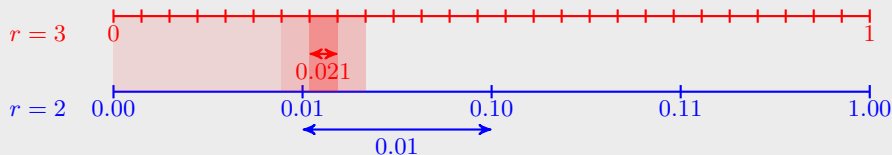
for all  $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

## Example

$X = 021\dots$

$Y = 01\dots$



# Base conversion

We want a functional  $\Gamma : \Sigma_r^\infty \times \mathbb{N} \rightarrow \Sigma_s$  which converts from base  $r$  to base  $s$ :

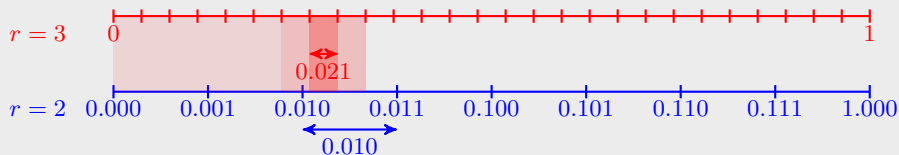
for all  $X \in \Sigma_r^\infty, Y \in \Sigma_s^\infty$

$$\Gamma^X \text{ is total and } \Gamma^X = Y \Rightarrow \langle 0.X \rangle_r = \langle 0.Y \rangle_s$$

## Example

$X = 021\dots$

$Y = 010\dots$



# Base conversion is not honest!

## Example

$X = \dots$

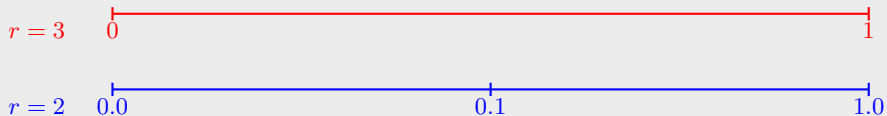
$Y = \dots$

# Base conversion is not honest!

## Example

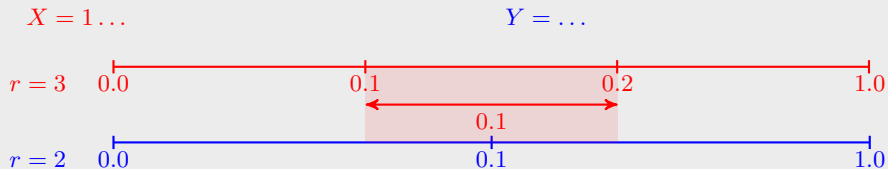
$X = \dots$

$Y = \dots$



# Base conversion is not honest!

Example



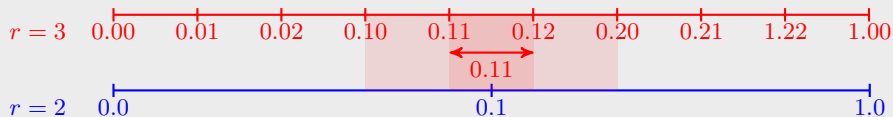


# Base conversion is not honest!

## Example

$X = 11\dots$

$Y = \dots$

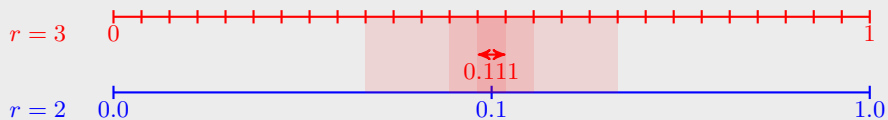


# Base conversion is not honest!

## Example

$X = 111\dots$

$Y = \dots$

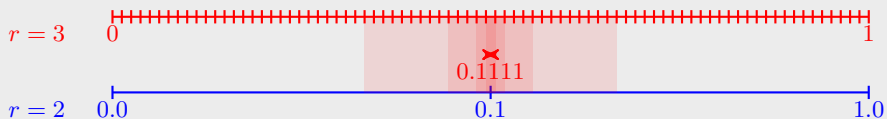


# Base conversion is not honest!

## Example

$$X = 1111 \dots$$

$$Y = \dots$$



So there is no such  $\Gamma$ .

## Base conversion with small error

For  $\tau \in \Sigma_s^*$  and  $i \in \mathbb{N}$ , let

- ▶  $\text{bc}_{s \text{ to } r}^-(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- ▶  $\text{bc}_{s \text{ to } r}^+(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

## Base conversion with small error

For  $\tau \in \Sigma_s^*$  and  $i \in \mathbb{N}$ , let

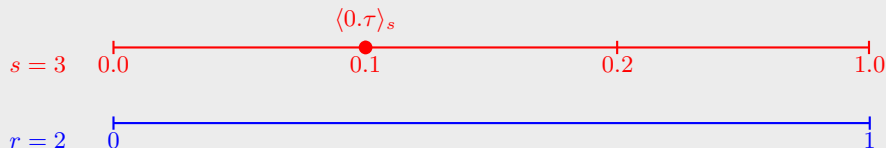
- ▶  $\text{bc}_{s \text{ to } r}^-(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- ▶  $\text{bc}_{s \text{ to } r}^+(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

### Example



## Base conversion with small error

For  $\tau \in \Sigma_s^*$  and  $i \in \mathbb{N}$ , let

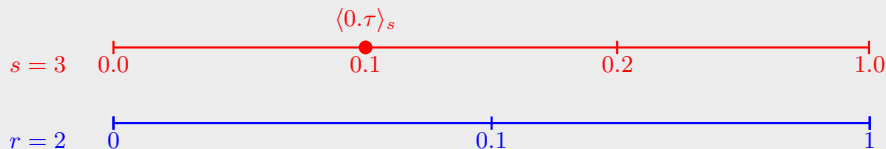
- ▶  $\text{bc}_{s \text{ to } r}^-(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- ▶  $\text{bc}_{s \text{ to } r}^+(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

### Example



## Base conversion with small error

For  $\tau \in \Sigma_s^*$  and  $i \in \mathbb{N}$ , let

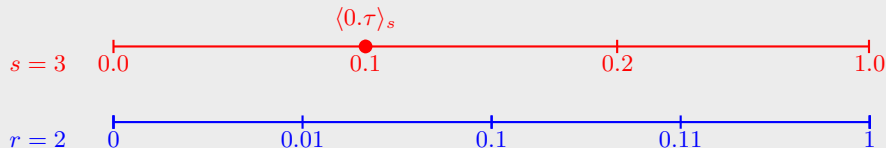
- ▶  $\text{bc}_{s \text{ to } r}^-(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- ▶  $\text{bc}_{s \text{ to } r}^+(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

### Example



## Base conversion with small error

For  $\tau \in \Sigma_s^*$  and  $i \in \mathbb{N}$ , let

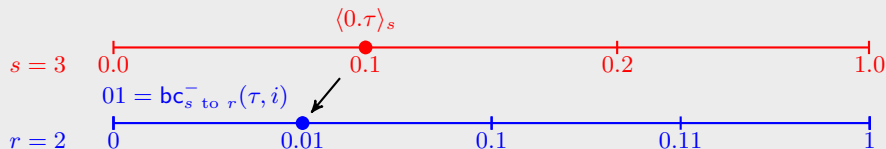
- ▶  $\text{bc}_{s \text{ to } r}^-(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- ▶  $\text{bc}_{s \text{ to } r}^+(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

### Example





## Base conversion with small error

For  $\tau \in \Sigma_s^*$  and  $i \in \mathbb{N}$ , let

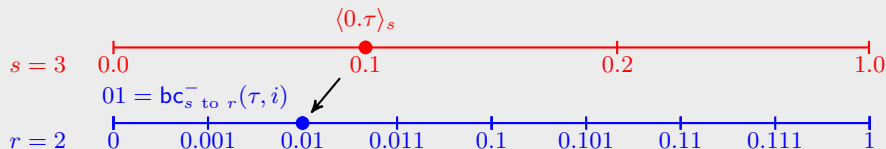
- ▶  $\text{bc}_{s \text{ to } r}^-(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- ▶  $\text{bc}_{s \text{ to } r}^+(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

### Example



## Base conversion with small error

For  $\tau \in \Sigma_s^*$  and  $i \in \mathbb{N}$ , let

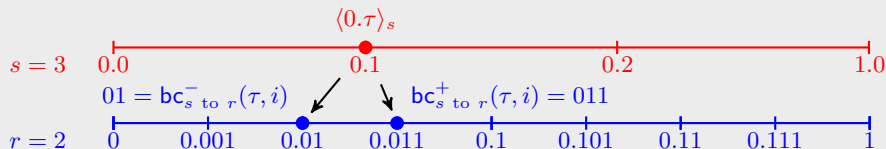
- ▶  $\text{bc}_{s \text{ to } r}^-(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- ▶  $\text{bc}_{s \text{ to } r}^+(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

### Example



# Base conversion with small error

For  $\tau \in \Sigma_s^*$  and  $i \in \mathbb{N}$ , let

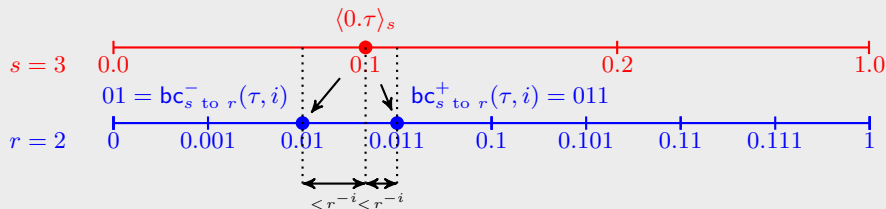
- ▶  $\text{bc}_{s \text{ to } r}^-(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r < r^{-i},$$

- ▶  $\text{bc}_{s \text{ to } r}^+(\tau, i)$  be the string  $\sigma$  in  $\Sigma_r^*$  of minimal length such that

$$0 \leq \langle 0.\sigma \rangle_r - \langle 0.\tau \rangle_s < r^{-i},$$

## Example



# Base conversion with small error

Approximation of a rational in base  $s$  with a rational in base  $r$

**input** :  $\tau \in \Sigma_s^*$  and  $i \in \mathbb{N}$

**output**:  $\sigma \in \Sigma_r^*$ ,  $\sigma = \text{bc}_{s \text{ to } r}^-(\tau, i)$

$\sigma := \emptyset$

**while**  $\langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r > r^{-i}$  **do**

    Find the largest  $x \in \Sigma_r$  such that  $\langle 0.\sigma \hat{x} \rangle_r \leq \langle 0.\tau \rangle_s$   
     $\sigma := \sigma \hat{x}$

# Base conversion with small error

## Approximation of a rational in base $s$ with a rational in base $r$

**input** :  $\tau \in \Sigma_s^*$  and  $i \in \mathbb{N}$   
**output**:  $\sigma \in \Sigma_r^*$ ,  $\sigma = \text{bc}_{s \text{ to } r}^-(\tau, i)$

$\sigma := \emptyset$

**while**  $\langle 0.\tau \rangle_s - \langle 0.\sigma \rangle_r > r^{-i}$  **do**

    Find the largest  $x \in \Sigma_r$  such that  $\langle 0.\sigma \hat{x} \rangle_r \leq \langle 0.\tau \rangle_s$   
     $\sigma := \sigma \hat{x}$

The time complexity of  $\text{bc}_{s \text{ to } r}^+$  or  $\text{bc}_{s \text{ to } r}^-$  on argument  $(\tau, i)$  is measured in  $n = |\tau| + i$ .

### Theorem

$\text{bc}_{s \text{ to } r}^-(\tau, i), \text{bc}_{s \text{ to } r}^+(\tau, i) \in \text{DTIME}(n^2)$ .

# Outline

Notation and definitions

Resource bounded versions of known results about martingales

Base conversion

Summary of Brattka, Miller, Nies 2011

Polynomial time randomness is base invariant

Polynomial time randomness and normality

# Martingales and analysis - Brattka, Miller, Nies 2011

Each martingale  $M$  in base  $r$  induces a measure  $\mu_M$  on the algebra of clopen sets defined by

$$\mu_M([\sigma]) = \frac{M(\sigma)}{r^{|\sigma|}}, \text{ for } \sigma \in \Sigma_r^*.$$

Via Carathéodory's extension theorem this measure can be extended to a Borel measure on Cantor space, and if  $\mu_M$  is atomless, we can also think of it as a Borel measure on  $[0, 1]$ :  $\mu_M$  is determined by

$$\mu_M(I_\sigma^r) = \frac{M(\sigma)}{r^{|\sigma|}},$$

where for any  $\sigma \in \Sigma_r^*$  we define

$$I_\sigma^r = \left[ \langle 0.\sigma \rangle_r, \langle 0.\sigma \rangle_r + r^{-|\sigma|} \right].$$

# Martingales and analysis - Brattka, Miller, Nies 2011

We say that a martingale is *atomless* if  $\mu_M$  is atomless.

## Fact

*If  $M$  has the savings property then  $M$  is atomless.*

The *cumulative distribution function associated with  $\mu_M$* , notated  $\text{cdf}_M(x) : [0, 1] \rightarrow [0, 1]$ , is defined by:

$$\text{cdf}_M(x) = \mu_M([0, x)).$$

## Fact

*If  $M$  is atomless then  $\text{cdf}_M$  is nondecreasing and continuous.*



# Martingales and analysis - Brattka, Miller, Nies 2011

If  $f$  is a nondecreasing function with domain containing  $[0, 1] \cap \mathbb{Q}$  and  $s$  is a base then  $\text{mart}_f^s : \Sigma_s^* \rightarrow \mathbb{R}$  is defined as follows:

$$\text{mart}_f^s(\tau) = \frac{f(\langle 0.\tau \rangle_s + s^{-|\tau|}) - f(\langle 0.\tau \rangle_s)}{s^{-|\tau|}}.$$

**Proposition (BMN 2011)**

$\text{mart}_f^s$  is a martingale in base  $s$ .

# Martingales and analysis - Brattka, Miller, Nies 2011

They established a correspondence between atomless martingales and nondecreasing continuous functions.

## Proposition (BMN 2011)

*Let  $s$  be a base and let  $f$  be a nondecreasing continuous function on  $[0, 1]$  such that  $f(0) = 0$ . Then  $\text{cdf}_{\text{mart}_f^s} = f$ .*

## Theorem (BMN 2011)

*Suppose  $M$  is a martingale in base  $r$  with the savings property, and  $z \in [0, 1]$  is not a rational in base  $r$ . Then  $M$  succeeds on the  $r$ -ary expansion of  $z$  iff*

$$\liminf_{h \rightarrow 0} \frac{\text{cdf}_M(z+h) - \text{cdf}_M(z)}{h} = \infty.$$

# Martingales and analysis - Brattka, Miller, Nies 2011

## Lemma (BMN 2011)

Suppose  $M$  is a martingale in base  $r$  with the savings property. Let  $N : \Sigma_s^* \rightarrow \mathbb{R}^{\geq 0}$  be the following martingale in base  $s$ :

$$N(\tau) = \text{mart}_{\text{cdf}_M}^s(\tau) = \frac{\text{cdf}_M(\langle 0.\tau \rangle_s + s^{-|\tau|}) - \text{cdf}_M(\langle 0.\tau \rangle_s)}{s^{-|\tau|}}.$$

Suppose  $X \in \Sigma_r^\infty$  and  $Y \in \Sigma_s^\infty$  are such that  $\langle 0.X \rangle_r \notin \text{Rat}_r$ ,  $\langle 0.Y \rangle_s \notin \text{Rat}_s$  and  $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$ . If  $M$  succeeds on  $X$  then  $N$  succeeds on  $Y$ .

## Theorem (BMN 2011)

Computable randomness is base invariant.

# Outline

Notation and definitions

Resource bounded versions of known results about martingales

Base conversion

Summary of Brattka, Miller, Nies 2011

**Polynomial time randomness is base invariant**

Polynomial time randomness and normality

# An 'almost Lipschitz' condition

## Proposition

*Let  $M$  be a martingale in base  $r$  with the savings property. Then there are constants  $k, \varepsilon > 0$  such that for every  $x, y \in [0, 1]$ , if  $y - x \leq \varepsilon$  then*

$$\text{cdf}_M(y) - \text{cdf}_M(x) \leq -k \cdot (y - x) \cdot \log(y - x).$$

# An 'almost Lipschitz' condition

## Proposition

Let  $M$  be a martingale in base  $r$  with the savings property. Then there are constants  $k, \varepsilon > 0$  such that for every  $x, y \in [0, 1]$ , if  $y - x \leq \varepsilon$  then

$$\text{cdf}_M(y) - \text{cdf}_M(x) \leq -k \cdot (y - x) \cdot \log(y - x).$$

## Proof.

- ▶ Let  $n \in \mathbb{N}$  be the least such that  $r^{-n} < y - x$
- ▶ Let  $p$  be the least of the form  $i \cdot r^{-n}$  such that  $x \leq p + r^{-n}$
- ▶ Let  $q$  be the minimum between 1 and  $(i + r + 1) \cdot r^{-n}$
- ▶  $y \leq q$ , and hence  $[x, y] \subseteq [p, q]$

$$\begin{aligned} \text{cdf}_M(y) - \text{cdf}_M(x) &\leq \text{cdf}_M(q) - \text{cdf}_M(p) \\ &= \mu_M[p, q] \\ &= \sum_{j=0}^{\min(r, r^n - i - 1)} \mu_M([(i + j) \cdot r^{-n}, (i + j + 1) \cdot r^{-n}]) \\ &\leq (r + 1) \cdot r^{-n} \cdot (c \cdot n + M(\emptyset)). \end{aligned}$$

- ▶  $r^{-(n-1)} \geq y - x \Rightarrow n \leq 1 - \log_r(y - x)$

# Computing $\text{cdf}_M$

## Lemma

Let  $M$  be a  $t(n)$ -martingale in base  $r$  with the savings property. Then  $\text{cdf}_M$  restricted to rationals in base  $r$  is a rational in base  $r$ . Also, for  $\sigma \in \Sigma_r^n$ ,  $\text{cdf}_M(\langle 0.\sigma \rangle_r) \in \text{DTIME}(n \cdot t(n))$  (output represented in base  $r$ ).

# Computing $\text{cdf}_M$

## Lemma

Let  $M$  be a  $t(n)$ -martingale in base  $r$  with the savings property. Then  $\text{cdf}_M$  restricted to rationals in base  $r$  is a rational in base  $r$ . Also, for  $\sigma \in \Sigma_r^n$ ,  $\text{cdf}_M(\langle 0.\sigma \rangle_r) \in \text{DTIME}(n \cdot t(n))$  (output represented in base  $r$ ).

## Proof.

Greedy computation of  $\text{cdf}_M(\langle 0.\sigma \rangle_r)$ :

$$\begin{aligned}\text{cdf}_M(\langle 0.\sigma \rangle_r) &= \mu_M([0, \langle 0.\sigma \rangle_r]) \\ &= \sum_{i=0}^{n-1} \sum_{b=0}^{\sigma^{(i)}-1} \mu_M(I_{(\sigma \upharpoonright_i) \frown b}^r) \\ &= \sum_{i=0}^{n-1} \sum_{b=0}^{\sigma^{(i)}-1} \frac{M((\sigma \upharpoonright_i) \frown b)}{r^{i+1}}\end{aligned}$$

$\text{cdf}_M$  is computable in time  $O(n \cdot t(n))$ .



# Computing $\text{cdf}_M$

## Lemma

Let  $M$  be a  $t(n)$ -martingale in base  $r$  with the savings property. Then  $\text{cdf}_M$  restricted to rationals in base  $r$  is a rational in base  $r$ . Also, for  $\sigma \in \Sigma_r^n$ ,  $\text{cdf}_M(\langle 0.\sigma \rangle_r) \in \text{DTIME}(n \cdot t(n))$  (output represented in base  $r$ ).

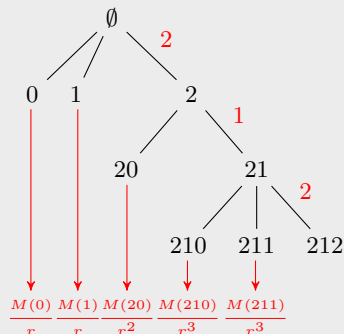
## Proof.

Greedy computation of  $\text{cdf}_M(\langle 0.\sigma \rangle_r)$ :

$$\begin{aligned}\text{cdf}_M(\langle 0.\sigma \rangle_r) &= \mu_M([0, \langle 0.\sigma \rangle_r]) \\ &= \sum_{i=0}^{n-1} \sum_{b=0}^{\sigma(i)-1} \mu_M(I_{(\sigma|_i) \frown b}^r) \\ &= \sum_{i=0}^{n-1} \sum_{b=0}^{\sigma(i)-1} \frac{M((\sigma|_i) \frown b)}{r^{i+1}}\end{aligned}$$

$\text{cdf}_M$  is computable in time  $O(n \cdot t(n))$ .

Example.  $\sigma = 212$ ,  $r = 3$



# Polynomial time randomness is base invariant

For  $M$  a martingale in base  $r$  and  $N$  a martingale in base  $s$ , we say that  $N$  is an  $r$  to  $s$  base conversion of  $M$  in case the following holds: if  $M$  succeeds on  $X \in \Sigma_r^\infty$ , and  $Y \in \Sigma_s^\infty$  is such that  $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$ , then  $N$  succeeds on  $Y$ .

**Lemma (Figueira, Nies 2013)**

*For any  $t(n)$ -martingale  $M$  in base  $r$  with the savings property there is a (real-valued) martingale  $N$  in base  $s$  such that:*

- ▶  $N$  is an  $r$  to  $s$  base conversion of  $M$ , and
- ▶  $N$  has an  $n \cdot t(n)$ -computable approximation.

# Polynomial time randomness is base invariant

Theorem (Figueira, Nies 2013)

*Let  $k \geq 1$ . If  $Y \in \Sigma_s^\infty$  is  $n^{k+3}$ -random in base  $s$  and  $X \in \Sigma_r^\infty$  is such that  $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$  then  $X$  is  $n^k$ -random in base  $r$ . In particular, polynomial time randomness is base invariant.*

# Polynomial time randomness is base invariant

Theorem (Figueira, Nies 2013)

*Let  $k \geq 1$ . If  $Y \in \Sigma_s^\infty$  is  $n^{k+3}$ -random in base  $s$  and  $X \in \Sigma_r^\infty$  is such that  $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$  then  $X$  is  $n^k$ -random in base  $r$ . In particular, polynomial time randomness is base invariant.*

Proof.

- ▶ Suppose that  $X \in \Sigma_r^\infty$  is not  $n^k$ -random in base  $r$

# Polynomial time randomness is base invariant

## Theorem (Figueira, Nies 2013)

*Let  $k \geq 1$ . If  $Y \in \Sigma_s^\infty$  is  $n^{k+3}$ -random in base  $s$  and  $X \in \Sigma_r^\infty$  is such that  $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$  then  $X$  is  $n^k$ -random in base  $r$ . In particular, polynomial time randomness is base invariant.*

## Proof.

- ▶ Suppose that  $X \in \Sigma_r^\infty$  is not  $n^k$ -random in base  $r$
- ▶ Let  $M$  be an  $n^k$ -martingale in base  $r$  which succeeds on  $X$

# Polynomial time randomness is base invariant

Theorem (Figueira, Nies 2013)

*Let  $k \geq 1$ . If  $Y \in \Sigma_s^\infty$  is  $n^{k+3}$ -random in base  $s$  and  $X \in \Sigma_r^\infty$  is such that  $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$  then  $X$  is  $n^k$ -random in base  $r$ . In particular, polynomial time randomness is base invariant.*

Proof.

- ▶ Suppose that  $X \in \Sigma_r^\infty$  is not  $n^k$ -random in base  $r$
- ▶ Let  $M$  be an  $n^k$ -martingale in base  $r$  which succeeds on  $X$
- ▶ There is a  $n^{k+1}$ -martingale  $\widetilde{M}$  in base  $r$  with the savings property such that  $\widetilde{M}$  succeeds on  $X$

# Polynomial time randomness is base invariant

Theorem (Figueira, Nies 2013)

Let  $k \geq 1$ . If  $Y \in \Sigma_s^\infty$  is  $n^{k+3}$ -random in base  $s$  and  $X \in \Sigma_r^\infty$  is such that  $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$  then  $X$  is  $n^k$ -random in base  $r$ . In particular, polynomial time randomness is base invariant.

Proof.

- ▶ Suppose that  $X \in \Sigma_r^\infty$  is not  $n^k$ -random in base  $r$
- ▶ Let  $M$  be an  $n^k$ -martingale in base  $r$  which succeeds on  $X$
- ▶ There is a  $n^{k+1}$ -martingale  $\widetilde{M}$  in base  $r$  with the savings property such that  $\widetilde{M}$  succeeds on  $X$
- ▶ By the lemma there is a (real-valued) martingale  $N$  in base  $s$  with an  $n^{k+2}$ -computable approximation, which is a base conversion of  $\widetilde{M}$ 
  - In particular  $N$  succeeds on  $Y$ .

# Polynomial time randomness is base invariant

Theorem (Figueira, Nies 2013)

Let  $k \geq 1$ . If  $Y \in \Sigma_s^\infty$  is  $n^{k+3}$ -random in base  $s$  and  $X \in \Sigma_r^\infty$  is such that  $\langle 0.X \rangle_r = \langle 0.Y \rangle_s$  then  $X$  is  $n^k$ -random in base  $r$ . In particular, polynomial time randomness is base invariant.

Proof.

- ▶ Suppose that  $X \in \Sigma_r^\infty$  is not  $n^k$ -random in base  $r$
- ▶ Let  $M$  be an  $n^k$ -martingale in base  $r$  which succeeds on  $X$
- ▶ There is a  $n^{k+1}$ -martingale  $\widetilde{M}$  in base  $r$  with the savings property such that  $\widetilde{M}$  succeeds on  $X$
- ▶ By the lemma there is a (real-valued) martingale  $N$  in base  $s$  with an  $n^{k+2}$ -computable approximation, which is a base conversion of  $\widetilde{M}$ 
  - In particular  $N$  succeeds on  $Y$ .
- ▶ There is an  $n^{k+3}$ -martingale  $\widetilde{N} \geq N$  in base  $s$

□



## Proof of the lemma

**Restatement.** Given  $M$  an  $n^k$ -martingale with the savings property in base  $r$ .  
Get an  $n^{k+1}$ -martingale  $N$  in base  $s$  such that

$M$  succeeds on a real  $\Rightarrow N$  succeeds on it

## Proof of the lemma

**Restatement.** Given  $M$  an  $n^k$ -martingale with the savings property in base  $r$ .  
Get an  $n^{k+1}$ -martingale  $N$  in base  $s$  such that

$M$  succeeds on a real  $\Rightarrow N$  succeeds on it

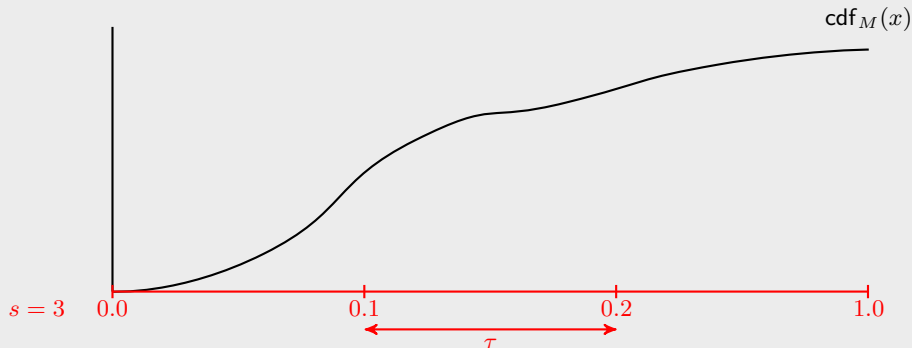
Define  $N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}$ ,  $p = \langle 0.\tau \rangle_s$ ,  $q = \langle 0.\tau \rangle_s + s^{-|\tau|}$

# Proof of the lemma

**Restatement.** Given  $M$  an  $n^k$ -martingale with the savings property in base  $r$ .  
Get an  $n^{k+1}$ -martingale  $N$  in base  $s$  such that

$M$  succeeds on a real  $\Rightarrow N$  succeeds on it

Define  $N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}$ ,  $p = \langle 0.\tau \rangle_s$ ,  $q = \langle 0.\tau \rangle_s + s^{-|\tau|}$

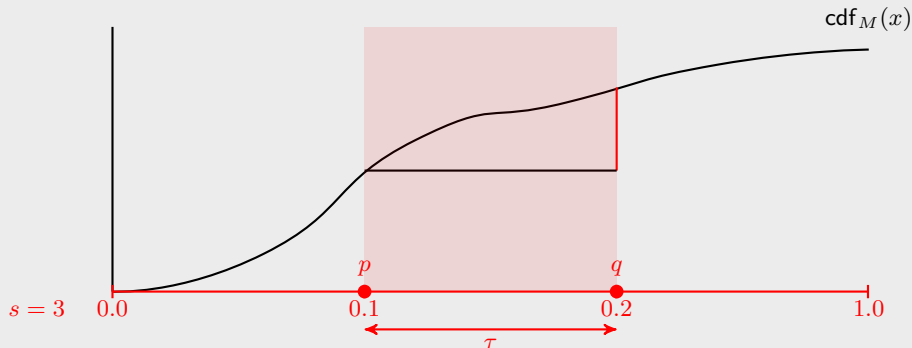


# Proof of the lemma

**Restatement.** Given  $M$  an  $n^k$ -martingale with the savings property in base  $r$ .  
Get an  $n^{k+1}$ -martingale  $N$  in base  $s$  such that

$M$  succeeds on a real  $\Rightarrow N$  succeeds on it

Define  $N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}$ ,  $p = \langle 0.\tau \rangle_s$ ,  $q = \langle 0.\tau \rangle_s + s^{-|\tau|}$

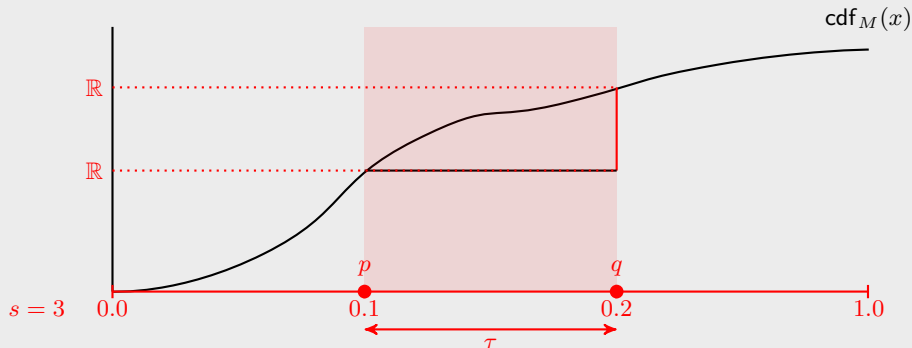


# Proof of the lemma

**Restatement.** Given  $M$  an  $n^k$ -martingale with the savings property in base  $r$ .  
Get an  $n^{k+1}$ -martingale  $N$  in base  $s$  such that

$M$  succeeds on a real  $\Rightarrow N$  succeeds on it

Define  $N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}$ ,  $p = \langle 0.\tau \rangle_s$ ,  $q = \langle 0.\tau \rangle_s + s^{-|\tau|}$



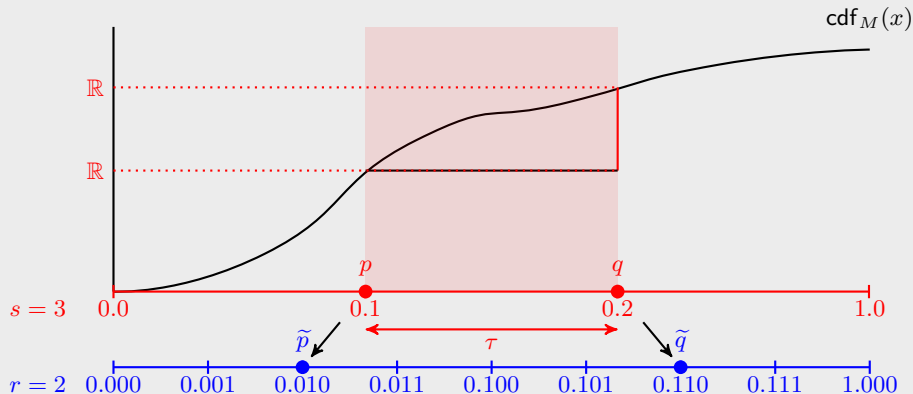
# Proof of the lemma

**Restatement.** Given  $M$  an  $n^k$ -martingale with the savings property in base  $r$ .  
Get an  $n^{k+1}$ -martingale  $N$  in base  $s$  such that

$M$  succeeds on a real  $\Rightarrow N$  succeeds on it

Define  $N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}$ ,  $p = \langle 0.\tau \rangle_s$ ,  $q = \langle 0.\tau \rangle_s + s^{-|\tau|}$

Approximate  $p, q \in \text{Rat}_s$  with  $\tilde{p}, \tilde{q} \in \text{Rat}_r$  resp.



# Proof of the lemma

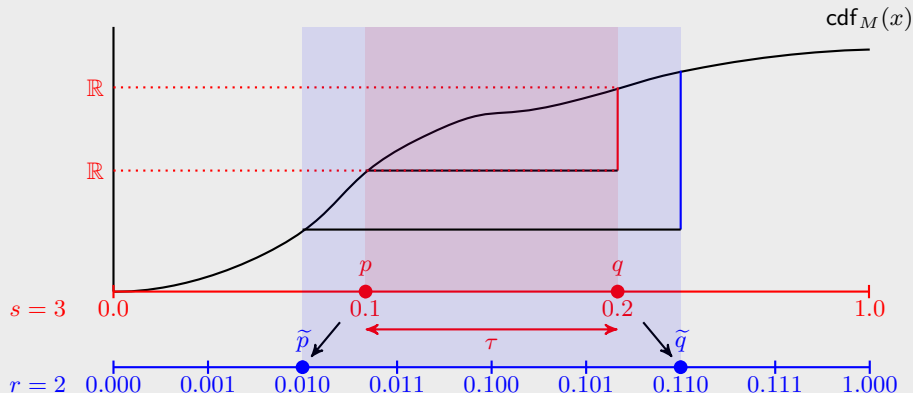
**Restatement.** Given  $M$  an  $n^k$ -martingale with the savings property in base  $r$ .  
Get an  $n^{k+1}$ -martingale  $N$  in base  $s$  such that

$M$  succeeds on a real  $\Rightarrow N$  succeeds on it

Define  $N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}$ ,  $p = \langle 0.\tau \rangle_s$ ,  $q = \langle 0.\tau \rangle_s + s^{-|\tau|}$

Approximate  $p, q \in \text{Rat}_s$  with  $\tilde{p}, \tilde{q} \in \text{Rat}_r$  resp.

Approximate  $\text{cdf}_M(q) - \text{cdf}_M(p)$  with  $\text{cdf}_M(\tilde{q}) - \text{cdf}_M(\tilde{p})$



# Proof of the lemma

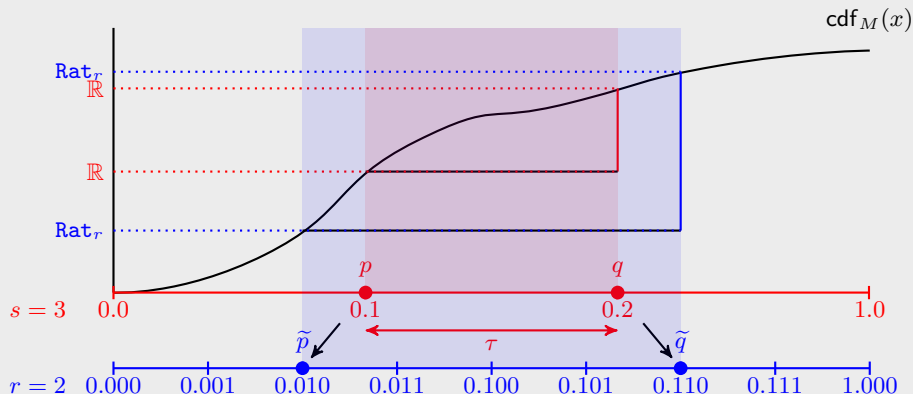
**Restatement.** Given  $M$  an  $n^k$ -martingale with the savings property in base  $r$ .  
Get an  $n^{k+1}$ -martingale  $N$  in base  $s$  such that

$M$  succeeds on a real  $\Rightarrow N$  succeeds on it

Define  $N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}$ ,  $p = \langle 0.\tau \rangle_s$ ,  $q = \langle 0.\tau \rangle_s + s^{-|\tau|}$

Approximate  $p, q \in \text{Rat}_s$  with  $\tilde{p}, \tilde{q} \in \text{Rat}_r$  resp.

Approximate  $\text{cdf}_M(q) - \text{cdf}_M(p)$  with  $\text{cdf}_M(\tilde{q}) - \text{cdf}_M(\tilde{p}) \in \text{Rat}_r$





# Proof of the lemma

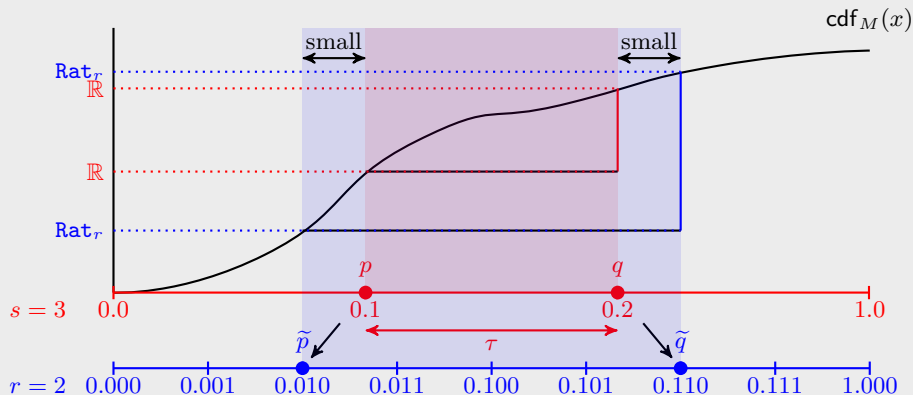
**Restatement.** Given  $M$  an  $n^k$ -martingale with the savings property in base  $r$ .  
Get an  $n^{k+1}$ -martingale  $N$  in base  $s$  such that

$M$  succeeds on a real  $\Rightarrow N$  succeeds on it

Define  $N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}$ ,  $p = \langle 0.\tau \rangle_s$ ,  $q = \langle 0.\tau \rangle_s + s^{-|\tau|}$

Approximate  $p, q \in \text{Rat}_s$  with  $\tilde{p}, \tilde{q} \in \text{Rat}_r$  resp.

Approximate  $\text{cdf}_M(q) - \text{cdf}_M(p)$  with  $\text{cdf}_M(\tilde{q}) - \text{cdf}_M(\tilde{p}) \in \text{Rat}_r$



# Proof of the lemma

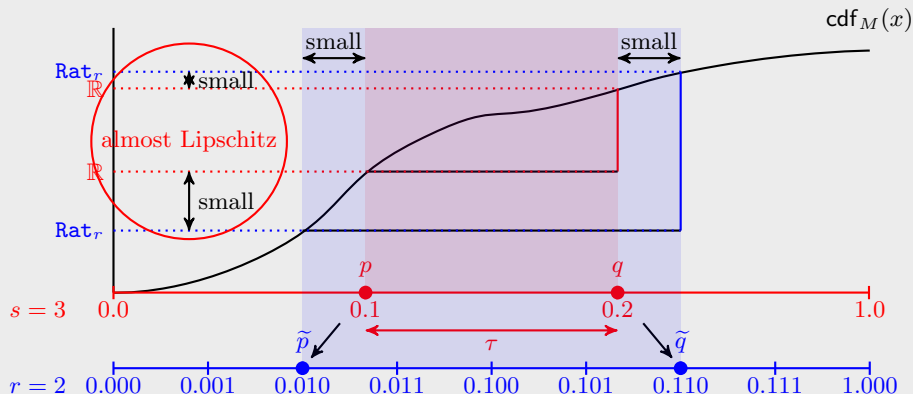
**Restatement.** Given  $M$  an  $n^k$ -martingale with the savings property in base  $r$ .  
Get an  $n^{k+1}$ -martingale  $N$  in base  $s$  such that

$M$  succeeds on a real  $\Rightarrow N$  succeeds on it

Define  $N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}$ ,  $p = \langle 0.\tau \rangle_s$ ,  $q = \langle 0.\tau \rangle_s + s^{-|\tau|}$

Approximate  $p, q \in \text{Rat}_s$  with  $\tilde{p}, \tilde{q} \in \text{Rat}_r$  resp.

Approximate  $\text{cdf}_M(q) - \text{cdf}_M(p)$  with  $\text{cdf}_M(\tilde{q}) - \text{cdf}_M(\tilde{p}) \in \text{Rat}_r$



## Proof of the lemma

Given an  $n^k$ -martingale  $M$  in base  $r$  with the savings property, construct a computable approximation of

$$N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}, \quad p = \langle 0.\tau \rangle_s, \quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$$

## Proof of the lemma

Given an  $n^k$ -martingale  $M$  in base  $r$  with the savings property, construct a computable approximation of

$$N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}, \quad p = \langle 0.\tau \rangle_s, \quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$$

### Computable approximation of $N$ (idea)

Step 1.                      Approximate  $p$  with  $\tilde{p}$  and  $q$  with  $\tilde{q}$                        $O(n^2)$

## Proof of the lemma

Given an  $n^k$ -martingale  $M$  in base  $r$  with the savings property, construct a computable approximation of

$$N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}, \quad p = \langle 0.\tau \rangle_s, \quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$$

### Computable approximation of $N$ (idea)

Step 1.	Approximate $p$ with $\tilde{p}$ and $q$ with $\tilde{q}$	$O(n^2)$
Step 2.	Compute $\text{cdf}_M(\tilde{q}) - \text{cdf}_M(\tilde{p})$	$O(n^{k+1})$

## Proof of the lemma

Given an  $n^k$ -martingale  $M$  in base  $r$  with the savings property, construct a computable approximation of

$$N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}, \quad p = \langle 0.\tau \rangle_s, \quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$$

### Computable approximation of $N$ (idea)

Step 1.	Approximate $p$ with $\tilde{p}$ and $q$ with $\tilde{q}$	$O(n^2)$
Step 2.	Compute $\text{cdf}_M(\tilde{q}) - \text{cdf}_M(\tilde{p})$	$O(n^{k+1})$
Step 3.	Approximate $\text{cdf}_M(\tilde{q}) - \text{cdf}_M(\tilde{p})$ with rationals in base $s$	$O(n^2)$

## Proof of the lemma

Given an  $n^k$ -martingale  $M$  in base  $r$  with the savings property, construct a computable approximation of

$$N(\tau) = \frac{\text{cdf}_M(q) - \text{cdf}_M(p)}{s^{-|\tau|}}, \quad p = \langle 0.\tau \rangle_s, \quad q = \langle 0.\tau \rangle_s + s^{-|\tau|}$$

### Computable approximation of $N$ (idea)

Step 1.	Approximate $p$ with $\tilde{p}$ and $q$ with $\tilde{q}$	$O(n^2)$
Step 2.	Compute $\text{cdf}_M(\tilde{q}) - \text{cdf}_M(\tilde{p})$	$O(n^{k+1})$
Step 3.	Approximate $\text{cdf}_M(\tilde{q}) - \text{cdf}_M(\tilde{p})$ with rationals in base $s$	$O(n^2)$

In total, the computable approximation for  $N$  is  $O(n^{k+1})$

# Outline

Notation and definitions

Resource bounded versions of known results about martingales

Base conversion

Summary of Brattka, Miller, Nies 2011

Polynomial time randomness is base invariant

Polynomial time randomness and normality



## How much randomness is needed to be normal?

Schnorr (1971) showed that if  $Z \in \Sigma_2^\infty$  is  $n^2$ -random in base 2 then  $Z$  is simply normal in base 2. Then he concluded that  $n^2$ -randomness implies normality in base 2.

# How much randomness is needed to be normal?

Schnorr (1971) showed that if  $Z \in \Sigma_2^\infty$  is  $n^2$ -random in base 2 then  $Z$  is simply normal in base 2. Then he concluded that  $n^2$ -randomness implies normality in base 2.

We adapt Wang's (1996) version of Schnorr's proof that all  $n^2$ -random sequences in base 2 are simply normal in base 2

- ▶ normality instead of simply normality
- ▶ any base
- ▶ better complexity

**Theorem (Figueira, Nies 2013)**

*If  $Z$  is  $n \cdot \log^2 n$ -random in base  $r$  then  $Z$  is normal in base  $r$ .*

## $n \cdot \log^2 n$ -randomness implies normality

Choose the minimal string  $\alpha \hat{c}$  that violates normality, and choose a small  $\delta$

Suppose  $Z$  is not normal in base  $r$ .

Let  $c \in \Sigma_r$  and  $\alpha \in \Sigma_r^*$  such that  $\alpha \hat{c}$  is a string of minimal length for which it is not the case that  $\lim_{n \rightarrow \infty} \text{occ}_{\alpha \hat{c}}(Z \upharpoonright_n) / n = r^{-|\alpha|-1}$ . Define

$$\text{occ}_{\alpha \hat{c}}(\sigma) = \sum_{d \in \Sigma_r \setminus \{c\}} \text{occ}_{\alpha \hat{d}}(\sigma).$$

By the choice of  $\alpha$ , there is  $\varepsilon > 0$  such that one of the following is true:

$$(\exists^\infty n) \quad \frac{\text{occ}_{\alpha \hat{c}}(Z \upharpoonright_n)}{n} > r^{-|\alpha|-1} + \varepsilon \quad (1)$$

$$(\exists^\infty n) \quad \frac{\text{occ}_{\alpha \hat{c}}(Z \upharpoonright_n)}{n} < r^{-|\alpha|-1} - r\varepsilon. \quad (2)$$

Wlog we assume (1) holds. Let  $\delta$  be so that  $\delta / (r - 1) \in \text{Rat}_r^{\geq 0}$  and

$$\limsup_n \frac{\text{occ}_{\alpha \hat{c}}(Z \upharpoonright_n)}{n} > \frac{1 + \delta}{r^{|\alpha|+1}}.$$

## $n \cdot \log^2 n$ -randomness implies normality

Define the martingale  $L$  in terms of  $\delta$  and  $\alpha \hat{c}$

Let

$$p = 1 + \delta \quad \text{and} \quad q = 1 - \frac{\delta}{r-1}$$

Note that  $p, q \in \text{Rat}_r^{\geq 0}$ . Define  $L : \Sigma_r^* \rightarrow \text{Rat}_r^{\geq 0}$  as follows:

$$L(\lambda) = 1$$
$$L(\sigma \hat{b}) = \begin{cases} L(\sigma) & \text{if } \alpha \text{ is not a suffix of } \sigma \\ p \cdot L(\sigma) & \text{if } \alpha \text{ is a suffix of } \sigma, \text{ and } b = c \\ q \cdot L(\sigma) & \text{if } \alpha \text{ is a suffix of } \sigma, \text{ and } b \neq c \end{cases}$$

For all  $\sigma \in \Sigma_r^*$ :

$$L(\sigma) = p^{\text{occ}_{\alpha \hat{c}}(\sigma)} \cdot q^{\text{occ}_{\alpha \hat{e}}(\sigma)}.$$

**Fact**

$L$  is a  $\text{Rat}_r^{\geq 0}$ -valued martingale in base  $r$ .

# $n \cdot \log^2 n$ -randomness implies normality

$L$  succeeds

**Fact**

*L succeeds on Z.*

# $n \cdot \log^2 n$ -randomness implies normality

$L$  succeeds

## Fact

$L$  succeeds on  $Z$ .

## Proof.

Since  $\text{occ}_{\alpha \wedge \bar{c}}(\sigma) \leq \text{occ}_{\alpha}(\sigma) - \text{occ}_{\alpha \wedge c}(\sigma)$  and  $\log q$  is negative,

$$\begin{aligned} \log L(Z \upharpoonright_n) &\geq \text{occ}_{\alpha \wedge \bar{c}}(Z \upharpoonright_n) \cdot \log p + [\text{occ}_{\alpha}(Z \upharpoonright_n) - \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)] \cdot \log q \\ &= \text{occ}_{\alpha}(Z \upharpoonright_n) \cdot \log q + \text{occ}_{\alpha \wedge \bar{c}}(Z \upharpoonright_n) \cdot (\log p - \log q). \end{aligned}$$

# $n \cdot \log^2 n$ -randomness implies normality

$L$  succeeds

**Fact**

$L$  succeeds on  $Z$ .

**Proof.**

Since  $\text{occ}_{\alpha \wedge \bar{c}}(\sigma) \leq \text{occ}_{\alpha}(\sigma) - \text{occ}_{\alpha \wedge c}(\sigma)$  and  $\log q$  is negative,

$$\begin{aligned} \log L(Z \upharpoonright_n) &\geq \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n) \cdot \log p + [\text{occ}_{\alpha}(Z \upharpoonright_n) - \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)] \cdot \log q \\ &= \text{occ}_{\alpha}(Z \upharpoonright_n) \cdot \log q + \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n) \cdot (\log p - \log q). \end{aligned}$$

By taking the lim sup we obtain  $\limsup_n \frac{\log L(Z \upharpoonright_n)}{n} \geq$

$$\begin{aligned} &\limsup_n \frac{\text{occ}_{\alpha}(Z \upharpoonright_n)}{n} \cdot \log q + \frac{\text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)}{n} \cdot (\log p - \log q) \\ &= \frac{\log q}{r^{|\alpha|}} + (\log p - \log q) \cdot \limsup_n \frac{\text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)}{n} \quad (\text{minimality of } \alpha \wedge c) \\ &> \frac{\log q}{r^{|\alpha|}} + (\log p - \log q) \cdot \frac{1 + \delta}{r^{|\alpha|+1}} \quad (\text{by the choice of } \delta) \\ &= \frac{1}{r^{|\alpha|+1}} \cdot \left( (1 + \delta) \cdot \log(1 + \delta) + (r - 1 - \delta) \cdot \log\left(1 - \frac{\delta}{r - 1}\right) \right) = \ell \end{aligned}$$

# $n \cdot \log^2 n$ -randomness implies normality

$L$  succeeds

**Fact**

$L$  succeeds on  $Z$ .

**Proof.**

Since  $\text{occ}_{\alpha \wedge \bar{c}}(\sigma) \leq \text{occ}_{\alpha}(\sigma) - \text{occ}_{\alpha \wedge c}(\sigma)$  and  $\log q$  is negative,

$$\begin{aligned} \log L(Z \upharpoonright_n) &\geq \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n) \cdot \log p + [\text{occ}_{\alpha}(Z \upharpoonright_n) - \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)] \cdot \log q \\ &= \text{occ}_{\alpha}(Z \upharpoonright_n) \cdot \log q + \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n) \cdot (\log p - \log q). \end{aligned}$$

By taking the lim sup we obtain  $\limsup_n \frac{\log L(Z \upharpoonright_n)}{n} \geq$

$$\begin{aligned} &\limsup_n \frac{\text{occ}_{\alpha}(Z \upharpoonright_n)}{n} \cdot \log q + \frac{\text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)}{n} \cdot (\log p - \log q) \\ &= \frac{\log q}{r^{|\alpha|}} + (\log p - \log q) \cdot \limsup_n \frac{\text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)}{n} \quad (\text{minimality of } \alpha \wedge c) \\ &> \frac{\log q}{r^{|\alpha|}} + (\log p - \log q) \cdot \frac{1 + \delta}{r^{|\alpha|+1}} \quad (\text{by the choice of } \delta) \\ &= \frac{1}{r^{|\alpha|+1}} \cdot \left( (1 + \delta) \cdot \log(1 + \delta) + (r - 1 - \delta) \cdot \log\left(1 - \frac{\delta}{r - 1}\right) \right) = \ell \end{aligned}$$

Fact:  $(\forall \varepsilon \in (0, 1))(\forall x \geq 1) (1 + \varepsilon) \cdot \log(1 + \varepsilon) + (x - \varepsilon) \cdot \log(1 - \varepsilon/x) > 0$ .



# $n \cdot \log^2 n$ -randomness implies normality

$L$  succeeds

**Fact**

$L$  succeeds on  $Z$ .

**Proof.**

Since  $\text{occ}_{\alpha \wedge \bar{c}}(\sigma) \leq \text{occ}_{\alpha}(\sigma) - \text{occ}_{\alpha \wedge c}(\sigma)$  and  $\log q$  is negative,

$$\begin{aligned} \log L(Z \upharpoonright_n) &\geq \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n) \cdot \log p + [\text{occ}_{\alpha}(Z \upharpoonright_n) - \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)] \cdot \log q \\ &= \text{occ}_{\alpha}(Z \upharpoonright_n) \cdot \log q + \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n) \cdot (\log p - \log q). \end{aligned}$$

By taking the lim sup we obtain  $\limsup_n \frac{\log L(Z \upharpoonright_n)}{n} \geq$

$$\begin{aligned} &\limsup_n \frac{\text{occ}_{\alpha}(Z \upharpoonright_n)}{n} \cdot \log q + \frac{\text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)}{n} \cdot (\log p - \log q) \\ &= \frac{\log q}{r^{|\alpha|}} + (\log p - \log q) \cdot \limsup_n \frac{\text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)}{n} \quad (\text{minimality of } \alpha \wedge c) \\ &> \frac{\log q}{r^{|\alpha|}} + (\log p - \log q) \cdot \frac{1 + \delta}{r^{|\alpha|+1}} \quad (\text{by the choice of } \delta) \\ &= \frac{1}{r^{|\alpha|+1}} \cdot \left( (1 + \delta) \cdot \log(1 + \delta) + (r - 1 - \delta) \cdot \log\left(1 - \frac{\delta}{r - 1}\right) \right) = \ell > 0 \end{aligned}$$

Fact:  $(\forall \varepsilon \in (0, 1))(\forall x \geq 1) (1 + \varepsilon) \cdot \log(1 + \varepsilon) + (x - \varepsilon) \cdot \log(1 - \varepsilon/x) > 0$ .

# $n \cdot \log^2 n$ -randomness implies normality

$L$  succeeds

**Fact**

$L$  succeeds on  $Z$ .

**Proof.**

Since  $\text{occ}_{\alpha \wedge \bar{c}}(\sigma) \leq \text{occ}_{\alpha}(\sigma) - \text{occ}_{\alpha \wedge c}(\sigma)$  and  $\log q$  is negative,

$$\begin{aligned}\log L(Z \upharpoonright_n) &\geq \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n) \cdot \log p + [\text{occ}_{\alpha}(Z \upharpoonright_n) - \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)] \cdot \log q \\ &= \text{occ}_{\alpha}(Z \upharpoonright_n) \cdot \log q + \text{occ}_{\alpha \wedge c}(Z \upharpoonright_n) \cdot (\log p - \log q).\end{aligned}$$

By taking the lim sup we obtain  $\limsup_n \frac{\log L(Z \upharpoonright_n)}{n} \geq$

$$\begin{aligned}&\limsup_n \frac{\text{occ}_{\alpha}(Z \upharpoonright_n)}{n} \cdot \log q + \frac{\text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)}{n} \cdot (\log p - \log q) \\ &= \frac{\log q}{r^{|\alpha|}} + (\log p - \log q) \cdot \limsup_n \frac{\text{occ}_{\alpha \wedge c}(Z \upharpoonright_n)}{n} \quad (\text{minimality of } \alpha \wedge c) \\ &> \frac{\log q}{r^{|\alpha|}} + (\log p - \log q) \cdot \frac{1 + \delta}{r^{|\alpha|+1}} \quad (\text{by the choice of } \delta) \\ &= \frac{1}{r^{|\alpha|+1}} \cdot \left( (1 + \delta) \cdot \log(1 + \delta) + (r - 1 - \delta) \cdot \log\left(1 - \frac{\delta}{r - 1}\right) \right) = \ell > 0\end{aligned}$$

Fact:  $(\forall \varepsilon \in (0, 1))(\forall x \geq 1) (1 + \varepsilon) \cdot \log(1 + \varepsilon) + (x - \varepsilon) \cdot \log(1 - \varepsilon/x) > 0$ .

$(\exists^\infty n) \log L(Z \upharpoonright_n)/n > \ell$ , and so  $(\exists^\infty n) L(Z \upharpoonright_n) > 2^{\ell \cdot n}$ .

# $n \cdot \log^2 n$ -randomness implies normality

Complexity of  $L$

## Exponentiation by repeated squaring

Fix  $x \in \text{Rat}_r$ . Compute  $m \mapsto x^m$ .

$$x^m = \begin{cases} (x^2)^{\frac{m}{2}} & \text{if } m \text{ is even} \\ x \cdot (x^2)^{\frac{m-1}{2}} & \text{if } m \text{ is odd} \end{cases}$$

$O(\log n)$  recursive calls. In each call, a fixed number of  $+$  and  $\cdot$ .  
 $m \mapsto x^m \in \text{DTIME}(m \cdot \log^2 m)$ .

# $n \cdot \log^2 n$ -randomness implies normality

Complexity of  $L$

## Exponentiation by repeated squaring

Fix  $x \in \text{Rat}_r$ . Compute  $m \mapsto x^m$ .

$$x^m = \begin{cases} (x^2)^{\frac{m}{2}} & \text{if } m \text{ is even} \\ x \cdot (x^2)^{\frac{m-1}{2}} & \text{if } m \text{ is odd} \end{cases}$$

$O(\log n)$  recursive calls. In each call, a fixed number of  $+$  and  $\cdot$ .  
 $m \mapsto x^m \in \text{DTIME}(m \cdot \log^2 m)$ .

## Fact

$L$  is computable in time  $O(n \cdot \log^2 n)$ .

## Proof.

- ▶ Recall  $L(\sigma) = p^{\text{occ}_{\alpha \wedge c}(\sigma)} \cdot q^{\text{occ}_{\alpha \wedge \bar{c}}(\sigma)}$ . Let  $\sigma$  of length  $n$ .
- ▶  $\text{occ}_{\alpha \wedge c}(\sigma)$  and  $\text{occ}_{\alpha \wedge \bar{c}}(\sigma)$  can be computed in linear time
- ▶  $p^{\text{occ}_{\alpha \wedge c}(\sigma)}$  and  $q^{\text{occ}_{\alpha \wedge \bar{c}}(\sigma)}$  can be computed in time  $n \cdot \log^2 n$
- ▶ The size of  $p^{\text{occ}_{\alpha \wedge c}(\sigma)}$  and  $q^{\text{occ}_{\alpha \wedge \bar{c}}(\sigma)}$  are  $O(n)$
- ▶ Multiplying  $p^{\text{occ}_{\alpha \wedge c}(\sigma)}$  and  $q^{\text{occ}_{\alpha \wedge \bar{c}}(\sigma)}$  can be done in  $O(n \cdot \log n^2)$

# Supermartingales

## Definition

A *supermartingale in base  $r$*  is a function  $M : \Sigma_r^* \rightarrow \mathbb{R}^{\geq 0}$  such that

$$(\forall \sigma \in \Sigma_r^*) \quad r \cdot M(\sigma) \geq \sum_{b \in \Sigma_r} M(\sigma \hat{\ } b)$$

# Supermartingales

## Definition

A *supermartingale in base  $r$*  is a function  $M : \Sigma_r^* \rightarrow \mathbb{R}^{\geq 0}$  such that

$$(\forall \sigma \in \Sigma_r^*) \quad r \cdot M(\sigma) \geq \sum_{b \in \Sigma_r} M(\sigma \hat{\ } b)$$

## Lemma

If  $M$  is a martingale in base  $r$  with a  $t(n)$ -computable approximation then there is a  $t(n)$ -supermartingale  $N$  in base  $r$  such that  $N \geq M$ .

## Lemma

For every  $t(n)$ -supermartingale  $M$  in base  $r$  there is an  $n \cdot t(n)$ -martingale  $N$  in base  $r$  such that  $N \geq M$ .

# How much randomness is needed to be abs. normal?

Proposition (Figueira, Nies 2013)

*If  $Z \in \Sigma_r^\infty$  is not normal in base  $r$  then there is an  $n^2$ -martingale with the savings property that succeeds on  $Z$ .*

# How much randomness is needed to be abs. normal?

## Proposition (Figueira, Nies 2013)

*If  $Z \in \Sigma_r^\infty$  is not normal in base  $r$  then there is an  $n^2$ -martingale with the savings property that succeeds on  $Z$ .*

## Corollary

*Suppose  $Z \in \Sigma_r^\infty$  is such that no  $n^3$ -supermartingale in base  $r$  succeeds on  $Z$ . Then  $z = \langle 0.Z \rangle_r$  is absolutely normal. In particular, if  $Z$  is  $n^4$ -random in base  $r$  then  $z$  is absolutely normal.*



# How much randomness is needed to be abs. normal?

## Proposition (Figueira, Nies 2013)

*If  $Z \in \Sigma_r^\infty$  is not normal in base  $r$  then there is an  $n^2$ -martingale with the savings property that succeeds on  $Z$ .*

## Corollary

*Suppose  $Z \in \Sigma_r^\infty$  is such that no  $n^3$ -supermartingale in base  $r$  succeeds on  $Z$ . Then  $z = \langle 0.Z \rangle_r$  is absolutely normal. In particular, if  $Z$  is  $n^4$ -random in base  $r$  then  $z$  is absolutely normal.*

## Proof.

- ▶ Suppose  $Y \in \Sigma_s^\infty$  s.t.  $z = \langle 0.Y \rangle_s$  and  $Y$  is not normal in base  $s$

# How much randomness is needed to be abs. normal?

## Proposition (Figueira, Nies 2013)

*If  $Z \in \Sigma_r^\infty$  is not normal in base  $r$  then there is an  $n^2$ -martingale with the savings property that succeeds on  $Z$ .*

## Corollary

*Suppose  $Z \in \Sigma_r^\infty$  is such that no  $n^3$ -supermartingale in base  $r$  succeeds on  $Z$ . Then  $z = \langle 0.Z \rangle_r$  is absolutely normal. In particular, if  $Z$  is  $n^4$ -random in base  $r$  then  $z$  is absolutely normal.*

## Proof.

- ▶ Suppose  $Y \in \Sigma_s^\infty$  s.t.  $z = \langle 0.Y \rangle_s$  and  $Y$  is not normal in base  $s$
- ▶ There is an  $n^2$ -martingale  $M$  in base  $s$  with the savings property that succeeds on  $Y$

# How much randomness is needed to be abs. normal?

## Proposition (Figueira, Nies 2013)

*If  $Z \in \Sigma_r^\infty$  is not normal in base  $r$  then there is an  $n^2$ -martingale with the savings property that succeeds on  $Z$ .*

## Corollary

*Suppose  $Z \in \Sigma_r^\infty$  is such that no  $n^3$ -supermartingale in base  $r$  succeeds on  $Z$ . Then  $z = \langle 0.Z \rangle_r$  is absolutely normal. In particular, if  $Z$  is  $n^4$ -random in base  $r$  then  $z$  is absolutely normal.*

## Proof.

- ▶ Suppose  $Y \in \Sigma_s^\infty$  s.t.  $z = \langle 0.Y \rangle_s$  and  $Y$  is not normal in base  $s$
- ▶ There is an  $n^2$ -martingale  $M$  in base  $s$  with the savings property that succeeds on  $Y$
- ▶ There is a martingale in base  $r$  with an  $n^3$ -computable approximation which succeeds on  $Z$

# How much randomness is needed to be abs. normal?

## Proposition (Figueira, Nies 2013)

*If  $Z \in \Sigma_r^\infty$  is not normal in base  $r$  then there is an  $n^2$ -martingale with the savings property that succeeds on  $Z$ .*

## Corollary

*Suppose  $Z \in \Sigma_r^\infty$  is such that no  $n^3$ -supermartingale in base  $r$  succeeds on  $Z$ . Then  $z = \langle 0.Z \rangle_r$  is absolutely normal. In particular, if  $Z$  is  $n^4$ -random in base  $r$  then  $z$  is absolutely normal.*

## Proof.

- ▶ Suppose  $Y \in \Sigma_s^\infty$  s.t.  $z = \langle 0.Y \rangle_s$  and  $Y$  is not normal in base  $s$
- ▶ There is an  $n^2$ -martingale  $M$  in base  $s$  with the savings property that succeeds on  $Y$
- ▶ There is a martingale in base  $r$  with an  $n^3$ -computable approximation which succeeds on  $Z$
- ▶ There is an  $n^3$ -supermartingale in base  $r$  which succeeds on  $Z$

# How much randomness is needed to be abs. normal?

## Proposition (Figueira, Nies 2013)

*If  $Z \in \Sigma_r^\infty$  is not normal in base  $r$  then there is an  $n^2$ -martingale with the savings property that succeeds on  $Z$ .*

## Corollary

*Suppose  $Z \in \Sigma_r^\infty$  is such that no  $n^3$ -supermartingale in base  $r$  succeeds on  $Z$ . Then  $z = \langle 0.Z \rangle_r$  is absolutely normal. In particular, if  $Z$  is  $n^4$ -random in base  $r$  then  $z$  is absolutely normal.*

## Proof.

- ▶ Suppose  $Y \in \Sigma_s^\infty$  s.t.  $z = \langle 0.Y \rangle_s$  and  $Y$  is not normal in base  $s$
- ▶ There is an  $n^2$ -martingale  $M$  in base  $s$  with the savings property that succeeds on  $Y$
- ▶ There is a martingale in base  $r$  with an  $n^3$ -computable approximation which succeeds on  $Z$
- ▶ There is an  $n^3$ -supermartingale in base  $r$  which succeeds on  $Z$
- ▶ There is an  $n^4$ -martingale in base  $r$  which succeeds on  $Z$

# How to construct a $t(n)$ -random sequence $Z$ in 3 steps

1. Enumerate in  $(G_i)_{i \in \mathbb{N}}$  all  $t(n)$ -supermartingales in base  $r$  with initial capital 1

We may view  $\Phi_i$  as a partial function  $\Sigma_r^* \rightarrow \mathbf{Rat}_r^{\geq 0}$ .

Fix a time constructible nondecreasing and unbounded function  $h$ .

Let

$$\tilde{\Phi}_i(\sigma) = \begin{cases} \Phi_i(\sigma)[h(|i|) \cdot t(|\sigma|)] & \text{if } \Phi_i(\sigma)[h(|i|) \cdot t(|\sigma|)] \downarrow \\ 0 & \text{otherwise} \end{cases}$$

# How to construct a $t(n)$ -random sequence $Z$ in 3 steps

1. Enumerate in  $(G_i)_{i \in \mathbb{N}}$  all  $t(n)$ -supermartingales in base  $r$  with initial capital 1

We may view  $\Phi_i$  as a partial function  $\Sigma_r^* \rightarrow \text{Rat}_r^{\geq 0}$ .

Fix a time constructible nondecreasing and unbounded function  $h$ .

Let

$$\tilde{\Phi}_i(\sigma) = \begin{cases} \Phi_i(\sigma)[h(|i|) \cdot t(|\sigma|)] & \text{if } \Phi_i(\sigma)[h(|i|) \cdot t(|\sigma|)] \downarrow \\ 0 & \text{otherwise} \end{cases}$$

Define  $G : \mathbb{N} \times \Sigma_r^* \rightarrow \text{Rat}_r^{\geq 0}$  as follows:

$$G(i, \sigma) = \begin{cases} 1 & \text{if } \sigma = \emptyset \\ \tilde{\Phi}_i(\sigma) & \text{if } \sigma = \tau \hat{\ } b \text{ for } b \in \Sigma_r, \text{ and } \sum_{j \in \Sigma_r} \tilde{\Phi}_i(\tau \hat{\ } j) \leq r \cdot G(i, \tau) \\ 0 & \text{otherwise} \end{cases}$$

Let  $G_i(\sigma) = G(i, \sigma)$ , and  $p(x) = x \cdot \log x$ .

# How to construct a $t(n)$ -random sequence $Z$ in 3 steps

1. Enumerate in  $(G_i)_{i \in \mathbb{N}}$  all  $t(n)$ -supermartingales in base  $r$  with initial capital 1

We may view  $\Phi_i$  as a partial function  $\Sigma_r^* \rightarrow \text{Rat}_r^{\geq 0}$ .

Fix a time constructible nondecreasing and unbounded function  $h$ .

Let

$$\tilde{\Phi}_i(\sigma) = \begin{cases} \Phi_i(\sigma)[h(|i|) \cdot t(|\sigma|)] & \text{if } \Phi_i(\sigma)[h(|i|) \cdot t(|\sigma|)] \downarrow \\ 0 & \text{otherwise} \end{cases}$$

Define  $G : \mathbb{N} \times \Sigma_r^* \rightarrow \text{Rat}_r^{\geq 0}$  as follows:

$$G(i, \sigma) = \begin{cases} 1 & \text{if } \sigma = \emptyset \\ \tilde{\Phi}_i(\sigma) & \text{if } \sigma = \tau \hat{\ } b \text{ for } b \in \Sigma_r, \text{ and } \sum_{j \in \Sigma_r} \tilde{\Phi}_i(\tau \hat{\ } j) \leq r \cdot G(i, \tau) \\ 0 & \text{otherwise} \end{cases}$$

Let  $G_i(\sigma) = G(i, \sigma)$ , and  $p(x) = x \cdot \log x$ .

## Fact

- ▶  $G_i$  is a  $\text{Rat}_r^{\geq}$ -valued supermartingale in base  $r$  with  $G_i(\emptyset) = 1$
- ▶  $G(i, \sigma)$  is computed in time  $O(|\sigma| \cdot p(t'(|\sigma|)))$ , for  $t' \approx t$
- ▶ Suppose  $F$  is a  $t(n)$ -supermartingale such that  $F(\emptyset) = 1$ . Then there is  $e$  such that  $F = G_e$ .



## How to construct a $t(n)$ -random sequence $Z$ in 3 steps

2. Define a  $\text{Rat}_r$ -valued supermartingale  $H$  as a combination of all  $(G_i)_{i \in \mathbb{N}}$

Define  $\widehat{G}_i : \Sigma_r^* \rightarrow \mathbb{R}^{\geq 0}$  by

$$\widehat{G}_i(\sigma) = \begin{cases} r^{-i} - r^{-(i+1)} & \text{if } |\sigma| \leq r^i \\ r^{-2r^i} \cdot G_i(\sigma) & \text{otherwise} \end{cases}$$

**Fact**

$\widehat{G}_i$  is a supermartingale in base  $r$ .

# How to construct a $t(n)$ -random sequence $Z$ in 3 steps

2. Define a  $\text{Rat}_r$ -valued supermartingale  $H$  as a combination of all  $(G_i)_{i \in \mathbb{N}}$

Define  $\widehat{G}_i : \Sigma_r^* \rightarrow \mathbb{R}^{\geq 0}$  by

$$\widehat{G}_i(\sigma) = \begin{cases} r^{-i} - r^{-(i+1)} & \text{if } |\sigma| \leq r^i \\ r^{-2r^i} \cdot G_i(\sigma) & \text{otherwise} \end{cases}$$

**Fact**

$\widehat{G}_i$  is a supermartingale in base  $r$ .

Define

$$H(\sigma) = \sum_i \widehat{G}_i(\sigma).$$

If  $|\sigma| \leq r^0$  then  $H(\sigma) = 1$ , and if  $r^j < |\sigma| \leq r^{j+1}$  then

$$H(\sigma) = r^{-(j+1)} + \sum_{i \leq j} r^{-2r^i} \cdot G_i(\sigma). \quad (3)$$

# How to construct a $t(n)$ -random sequence $Z$ in 3 steps

2. Define a  $\text{Rat}_r$ -valued supermartingale  $H$  as a combination of all  $(G_i)_{i \in \mathbb{N}}$

Define  $\widehat{G}_i : \Sigma_r^* \rightarrow \mathbb{R}^{\geq 0}$  by

$$\widehat{G}_i(\sigma) = \begin{cases} r^{-i} - r^{-(i+1)} & \text{if } |\sigma| \leq r^i \\ r^{-2r^i} \cdot G_i(\sigma) & \text{otherwise} \end{cases}$$

**Fact**

$\widehat{G}_i$  is a supermartingale in base  $r$ .

Define

$$H(\sigma) = \sum_i \widehat{G}_i(\sigma).$$

If  $|\sigma| \leq r^0$  then  $H(\sigma) = 1$ , and if  $r^j < |\sigma| \leq r^{j+1}$  then

$$H(\sigma) = r^{-(j+1)} + \sum_{i \leq j} r^{-2r^i} \cdot G_i(\sigma). \quad (3)$$

**Fact**

- ▶  $H$  is a supermartingale, and by (3), it is  $\text{Rat}_r^{\geq 0}$ -valued.
- ▶ If  $\sigma \in \Sigma_r^n$  then  $H(\sigma) \in \text{DTIME}(n \cdot \log n \cdot p(t'(n)))$ .
- ▶ if  $F$  is a  $t(n)$ -supermartingale in base  $r$  then there are  $c, d > 0$  such that  $c + d \cdot F \leq H$ .

# How to construct a $t(n)$ -random sequence $Z$ in 3 steps

## 3. Compute the leftmost non-ascending path given by $H$

If  $Z \in \Sigma_r^\infty$  is such that  $\limsup_n H(Z \upharpoonright_n) < \infty$  then no  $t(n)$ -supermartingale in base  $r$  succeeds on  $Z$ .

$Z = \bigcap_n [\zeta_n] =$  Leftmost non-ascending path given by  $H$

**input** :  $n \in \mathbb{N}$

**output**:  $\zeta_n \in \Sigma_r^n$

$\zeta_n := \emptyset$

**for**  $i = 1$  to  $n$  **do**

    Find least  $b \in \Sigma_r$  such that  $H(\zeta_n) \geq H(\zeta_n \hat{\ } b)$

$\zeta_n := \zeta_n \hat{\ } b$

# How to construct a $t(n)$ -random sequence $Z$ in 3 steps

## 3. Compute the leftmost non-ascending path given by $H$

If  $Z \in \Sigma_r^\infty$  is such that  $\limsup_n H(Z \upharpoonright_n) < \infty$  then no  $t(n)$ -supermartingale in base  $r$  succeeds on  $Z$ .

$Z = \bigcap_n [\zeta_n] =$  Leftmost non-ascending path given by  $H$

**input** :  $n \in \mathbb{N}$

**output**:  $\zeta_n \in \Sigma_r^n$

$\zeta_n := \emptyset$

**for**  $i = 1$  to  $n$  **do**

    Find least  $b \in \Sigma_r$  such that  $H(\zeta_n) \geq H(\zeta_n \hat{\ } b)$   
     $\zeta_n := \zeta_n \hat{\ } b$

The complexity on input  $n$  is measured in  $n$ .

**Fact**

$n \mapsto Z \upharpoonright_n \in \text{DTIME}(n^2 \cdot \log n \cdot p(t'(n)))$ .

# An absolutely normal real in polynomial time

## Proposition

*There is  $Z \in \Sigma_r^\infty$  computable in time  $O(n^{k+2} \cdot \log^3 n)$  such that no  $n^k$ -supermartingale in base  $r$  succeeds on  $Z$ . In particular  $Z$  is  $n^k$ -random.*

## Proof.

The construction we have just seen with  $t(n) = n^k$  and  $h(n) = n$ . □

# An absolutely normal real in polynomial time

## Proposition

*There is  $Z \in \Sigma_r^\infty$  computable in time  $O(n^{k+2} \cdot \log^3 n)$  such that no  $n^k$ -supermartingale in base  $r$  succeeds on  $Z$ . In particular  $Z$  is  $n^k$ -random.*

## Proof.

The construction we have just seen with  $t(n) = n^k$  and  $h(n) = n$ . □

## Corollary

*There is  $Z \in \Sigma_r^\infty$  which is computable in time  $O(n^5 \cdot \log^3 n)$  such that  $\langle 0.Z \rangle_r$  is absolutely normal.*

## Proof.

- ▶ There is  $Z \in \Sigma_r^\infty$  which is computable in time  $O(n^5 \cdot \log^3 n)$  for which no  $n^3$ -supermartingale in base  $r$  succeeds on.
- ▶ If no  $n^3$ -supermartingale in base  $r$  succeeds on it then it is absolutely normal.

□

## Open questions

For many of our results it may be possibly to improve time bounds.

We showed a method for approximating rationals in a given base with rationals in another.

### Question

Is it possible to compute  $\text{bc}_{s,r}^-(\sigma)$  in less than quadratic time?

We showed that  $n^{k+3}$ -randomness in a given base implies  $n^k$ -randomness in another base.

### Question

Can we lower the '+3', or even show that  $n^k$ -randomness is base invariant (for large enough  $k$ )?

We showed that  $n \cdot \log^2 n$ -randomness implies normality.

### Question

Does linear-randomness in base  $r$  imply simple normality in base  $r$ , or even normality in base  $r$ ?



## Open questions

A sequence  $(y_j)_{j \in \mathbb{N}}$  of reals in  $[0, 1]$  is *uniformly distributed* if for each interval  $[u, v] \subseteq [0, 1]$ , the proportion of  $i < N$  with  $y_j \in [u, v]$  tends to  $v - u$  as  $N \rightarrow \infty$ , that is:

$$\lim_{N \rightarrow \infty} \frac{|\{j < N \mid y_j \in [u, v]\}|}{N} = v - u.$$

# Open questions

A sequence  $(y_j)_{j \in \mathbb{N}}$  of reals in  $[0, 1]$  is *uniformly distributed* if for each interval  $[u, v] \subseteq [0, 1]$ , the proportion of  $i < N$  with  $y_j \in [u, v]$  tends to  $v - u$  as  $N \rightarrow \infty$ , that is:

$$\lim_{N \rightarrow \infty} \frac{|\{j < N \mid y_j \in [u, v]\}|}{N} = v - u.$$

## Definition

Let  $r$  be a rational  $> 1$ . We say that  $x \in [0, 1]$  is *normal in base  $r$*  if the sequence  $(\{x \cdot r^n\})_{n \in \mathbb{N}}$  is uniformly distributed in  $[0, 1]$ .

For every  $r$  the set of reals normal for  $r$  has measure 1.

A real  $x$  is absolutely normal if it is normal in all integer bases  $> 1$ .

## Open questions

A sequence  $(y_j)_{j \in \mathbb{N}}$  of reals in  $[0, 1]$  is *uniformly distributed* if for each interval  $[u, v] \subseteq [0, 1]$ , the proportion of  $i < N$  with  $y_j \in [u, v]$  tends to  $v - u$  as  $N \rightarrow \infty$ , that is:

$$\lim_{N \rightarrow \infty} \frac{|\{j < N \mid y_j \in [u, v]\}|}{N} = v - u.$$

### Definition

Let  $r$  be a rational  $> 1$ . We say that  $x \in [0, 1]$  is *normal in base  $r$*  if the sequence  $(\{x \cdot r^n\})_{n \in \mathbb{N}}$  is uniformly distributed in  $[0, 1]$ .

For every  $r$  the set of reals normal for  $r$  has measure 1.

A real  $x$  is absolutely normal if it is normal in all integer bases  $> 1$ .

### Definition

$x$  is *rationally normal* if it is normal in all rational bases  $> 1$ .

# Open questions

Proposition (Special case of Brown, Moran and Pearce 1986)

*Rationally normal is stronger than absolutely normal.*

# Open questions

Proposition (Special case of Brown, Moran and Pearce 1986)

*Rationally normal is stronger than absolutely normal.*

Sets  $A, B \subseteq (1, \infty)$  are called *multiplicatively independent* (m.i.) if

$$\neg(\exists a \in A, b \in B, r, s \in \mathbb{N}) a^r = b^s$$

For instance,  $A = \mathbb{N} \setminus \{0, 1\}$  and  $B = \{3/2\}$  are m.i. BMP 1986:

*Given m.i. sets of algebraic numbers, every real is the sum of four numbers that are normal for all bases in  $A$ , but none in  $B$ .*

In particular, there are uncountably many reals that are absolutely normal, but not normal for the base  $3/2$ .

# Open questions

Proposition (Special case of Brown, Moran and Pearce 1986)

*Rationally normal is stronger than absolutely normal.*

Sets  $A, B \subseteq (1, \infty)$  are called *multiplicatively independent* (m.i.) if

$$\neg(\exists a \in A, b \in B, r, s \in \mathbb{N}) a^r = b^s$$

For instance,  $A = \mathbb{N} \setminus \{0, 1\}$  and  $B = \{3/2\}$  are m.i. BMP 1986:

*Given m.i. sets of algebraic numbers, every real is the sum of four numbers that are normal for all bases in  $A$ , but none in  $B$ .*

In particular, there are uncountably many reals that are absolutely normal, but not normal for the base  $3/2$ .

Conjecture

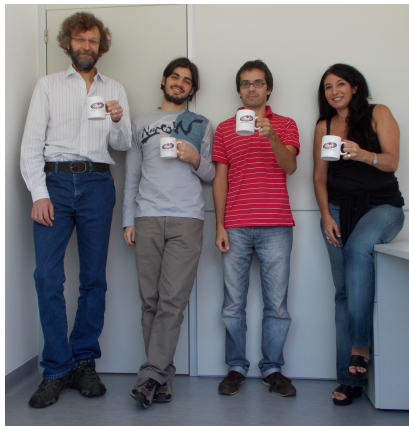
Every polynomial time random real is rationally normal.

In fact for some  $k$ ,  $n^k$ -random should imply rationally normal.

Question

What is the smallest such  $k$ ?

Fin



Colorín colorado, este cuento se ha  
acabado