Randomness and uniform distribution modulo one

Verónica Becher

Universidad de Buenos Aires & CONICET
LIA INFINIS

Joint work with Serge Grigorieff and Theodore Slaman

IRIF, Université Paris Diderot, January 19, 2018

How is randomness related to theory of uniform distribution?

Intuition for randomness

A real number is random if it belongs to not set of probability 0.

Intuition for randomness

A real number is random if it belongs to not set of probability 0.

A literal reading is not good: no real number would be random.

INFORMATION AND CONTROL 9, 602–619 (1966)

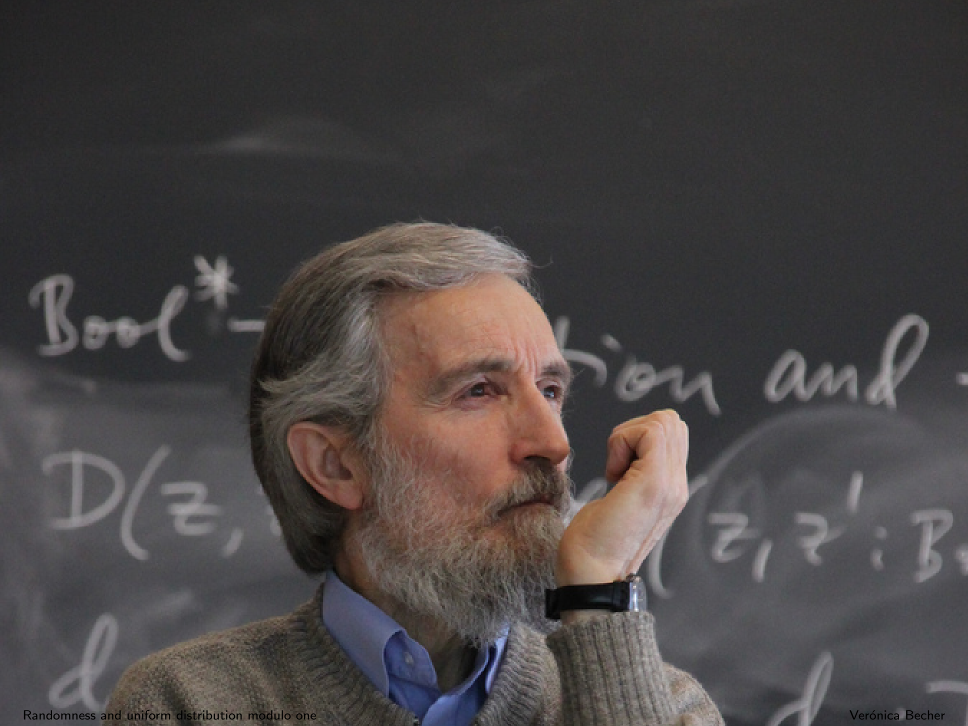
The Definition of Random Sequences

PER MARTIN-LÖF

Institute of Mathematical Statistics, University of Stockholm, Stockholm, Sweden

Kolmogorov has defined the conditional complexity of an object y when the object x is already given to us as the minimal length of a binary program which by means of x computes y on a certain asymptotically optimal machine. On the basis of this definition he has proposed to consider those elements of a given large finite population to be random whose complexity is maximal. Almost all elements of the population have a complexity which is close to the maximal value.

In this paper it is shown that the random elements as defined by Kolmogorov possess all conceivable statistical properties of randomness. They can equivalently be considered as the elements which withstand a certain universal stochasticity test. The definition is extended to infinite binary sequences and it is shown that the non random sequences form a maximal constructive null set. Finally, the Kollektivs introduced by von Mises obtain a definition which seems to satisfy all intuitive requirements.



Martin-Löf random reals

Definition (Martin-Löf 1966)

A real x is random if for every computable sequence $(V_n)_{n\geq 1}$ of computably enumerable open sets of reals such that $\mu(V_n) < 2^{-n}$,

$$x \notin \bigcap_{n\geq 1} V_n.$$

Martin-Löf random reals

Definition (Martin-Löf 1966)

A real x is random if for every computable sequence $(V_n)_{n \geq 1}$ of computably enumerable open sets of reals such that $\mu(V_n) < 2^{-n}$,

$$x \notin \bigcap_{n \geq 1} V_n.$$

Almost all (for Lebesgue measure) reals are random.

Random reals

A real number is random if, essentially, its initial segments can only be described explicitely by a Turing machine.

Random reals

A real number is random if, essentially, its initial segments can only be described explicitely by a Turing machine.

Definition (Chaitin 1975)

A real x is random if and only if $\exists C \; \forall n \; K(a_1 a_2..a_n) > n - C$, where K is the Kolmogorov complexity for a universal Turing machine with prefix-free domain.

Random reals

A real number is random if, essentially, its initial segments can only be described explicitly by a Turing machine.

Definition (Chaitin 1975)

A real x is random if and only if $\exists C\ \forall n\ K(a_1 a_2 .. a_n) > n - C$, where K is the Kolmogorov complexity for a universal Turing machine with prefix-free domain.

Theorem (Schnorr 1975)

Martin-Löf and Chaitin definitions coincide.

Examples of random reals

Chaitin's Ω numbers

Mathematische Annalen 77:313-352, 1916

Über die Gleichverteilung von Zahlen mod. Eins.*)

Von

Hermann Weyl in Zürich.

§ 1.

Grundlagen. Der lineare Fall.

Es seien auf der Geraden der reellen Zahlen unendlich viele Punkte

$$\alpha_1, \alpha_2, \alpha_3, \cdots$$

markiert; wir rollen die Gerade auf einen Kreis vom Umfange 1 auf und fragen, ob dabei die an den Stellen α_n befindlichen Marken schließlich

Uniform distribution modulo one

For a real x, $\{x\} = x - \lfloor x \rfloor$.

Definition

A sequence of reals $(x_n)_{n\geq 1}$ *is uniformly distributed modulo one, abbreviated u.d. mod* 1*, if for all* $a, b \in [0,1]$,

$$\lim_{N\to\infty} \frac{\#\big\{n : 1 \leq n \leq N, \{x_n\} \in [a,b)\big\}}{N} = b - a$$

Weyl's criterion

A sequence $(x_n)_{n\geq 1}$ of real numbers is u.d. mod 1 if for every Reimann integrable function f,

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(x_n) = \int_0^1 f(x)dx$$

Weyl's criterion

A sequence $(x_n)_{n\geq 1}$ of real numbers is u.d. mod 1 if for every Reimann integrable function f,

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(x_n) = \int_0^1 f(x)dx$$

Theorem (Weyl 1916)

A sequence $(x_n)_{n\geq 1}$ of real numbers is u.d. mod 1 if and only if for every non-zero integer h,

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} e^{2\pi i h x_n} = 0$$

Hermann Weyl on a seesaw at a Gasthaus in Nikolausberg, Germany in 1932

Examples

Theorem (Bohl; Sierpiński; Weyl 1909-1910)

A real x is irrational if and only if $(nx)_{n\geq 1}$ is u.d. mod 1.

Examples

Theorem (Bohl; Sierpiński; Weyl 1909-1910)

A real x is irrational if and only if $(nx)_{n\geq 1}$ is u.d. mod 1.

Theorem (Wall 1949)

A real x is Borel normal to base b if and only if $(b^n x)_{n\geq 1}$ is u.d. mod 1.

Koksma's General Metric Theorem

Given a real x in $[0,1]$ and $(u_n : [0,1] \to \mathbb{R})_{n\geq 1}$ consider $(u_n(x))_{n\geq 1}$.

Koksma's General Metric Theorem

Given a real x in $[0, 1]$ and $(u_n : [0, 1] \to \mathbb{R})_{n \geq 1}$ consider $(u_n(x))_{n \geq 1}$.

Definition (Koksma 1935)

Let $\mathcal{K}^{all}$ be the class of sequences $(u_n : [0, 1] \to \mathbb{R})_{n \geq 1}$ such that

1. $u_n(x)$ *is continuously differentiable for every* n*,*
2. $u'_m(x) - u'_n(x)$ *is monotone on* x *for all* $m \neq n$*,*
3. *there exists* $K > 0$ *such that for all* $x \in [0, 1]$ *and all* $m \neq n$*,* $|u'_m(x) - u'_n(x)| \geq K$*.*

Koksma's General Metric Theorem

Given a real x in $[0,1]$ and $(u_n : [0,1] \to \mathbb{R})_{n\geq 1}$ consider $(u_n(x))_{n\geq 1}$.

Definition (Koksma 1935)

Let $\mathcal{K}^{all}$ be the class of sequences $(u_n : [0,1] \to \mathbb{R})_{n\geq 1}$ such that

1. $u_n(x)$ *is continuously differentiable for every* n,
2. $u'_m(x) - u'_n(x)$ *is monotone on* x *for all* $m \neq n$,
3. *there exists* $K > 0$ *such that for all* $x \in [0,1]$ *and all* $m \neq n$, $|u'_m(x) - u'_n(x)| \geq K$.

Examples:
$(nx)_{n\geq 1}$

Koksma's General Metric Theorem

Given a real x in $[0,1]$ and $(u_n : [0,1] \to \mathbb{R})_{n\geq 1}$ consider $(u_n(x))_{n\geq 1}$.

Definition (Koksma 1935)

Let $\mathcal{K}^{all}$ be the class of sequences $(u_n : [0,1] \to \mathbb{R})_{n\geq 1}$ such that

1. $u_n(x)$ *is continuously differentiable for every* n*,*
2. $u'_m(x) - u'_n(x)$ *is monotone on* x *for all* $m \neq n$*,*
3. *there exists* $K > 0$ *such that for all* $x \in [0,1]$ *and all* $m \neq n$*,* $|u'_m(x) - u'_n(x)| \geq K$*.*

Examples:

$(nx)_{n\geq 1}$

$(2^n x)_{n\geq 1}$

Koksma's General Metric Theorem

Given a real x in $[0, 1]$ and $(u_n : [0, 1] \to \mathbb{R})_{n \geq 1}$ consider $(u_n(x))_{n \geq 1}$.

Definition (Koksma 1935)

Let $\mathcal{K}^{all}$ be the class of sequences $(u_n : [0, 1] \to \mathbb{R})_{n \geq 1}$ such that

1. $u_n(x)$ *is continuously differentiable for every* n,
2. $u'_m(x) - u'_n(x)$ *is monotone on* x *for all* $m \neq n$,
3. *there exists* $K > 0$ *such that for all* $x \in [0, 1]$ *and all* $m \neq n$, $|u'_m(x) - u'_n(x)| \geq K$.

Examples:

$(nx)_{n \geq 1}$

$(2^n x)_{n \geq 1}$

$(a_n x)_{n \geq 1}$ where $(a_n)_{n \geq 1}$ is a sequence of distinct integers.

Koksma's General Metric Theorem

Theorem (Koksma General Metric Theorem 1935)

Let $(u_n : [0,1] \to \mathbb{R})_{n\geq 1}$ *in* $\mathcal{K}^{all}$. *Then, for almost all (Lebesgue measure) reals* x *in* $[0,1]$, $(u_n(x))_{n\geq 1}$ *is u.d. mod* 1.

Avigad's Theorem

Theorem (Avigad 2013)

If a real x is random then for every computable sequence $(a_n)_{n\geq 1}$ of distinct integers, $(a_n x)_{n\geq 1}$ is u.d. mod 1.

Avigad's Theorem

Theorem (Avigad 2013)

If a real x is random then for every computable sequence $(a_n)_{n\geq 1}$ of distinct integers, $(a_n x)_{n\geq 1}$ is u.d. mod 1.

Actually Avigad's theorem holds for Schnorr randomness which is weaker than Martin-Löf randomness.

Effective Koksma class $\mathcal{K}$

Definition

Let $\mathcal{K}$ be the class of computable sequences $(u_n : [0,1] \to \mathbb{R})_{n \geq 1}$ in $\mathcal{K}^{all}$ such that the sequence of derivatives $(u'_n : [0,1] \to \mathbb{R})_{n \geq 1}$ is also computable.

Strict inclusion

Theorem 1

Let x be a real in $[0, 1]$. If x is random then for every $(u_n : [0, 1] \to \mathbb{R})_{n \geq 1}$ in $\mathcal{K}$ the sequence $(u_n(x))_{n \geq 1}$ is u.d. mod 1.

Strict inclusion

Theorem 1

Let x be a real in $[0,1]$. If x is random then for every $(u_n : [0,1] \to \mathbb{R})_{n\geq 1}$ in $\mathcal{K}$ the sequence $(u_n(x))_{n\geq 1}$ is u.d. mod 1.

The reverse of Theorem 1 does not hold.

Theorem 2

There is a real x in $[0,1]$ such that x is not random and for every $(u_n : [0,1] \to \mathbb{R})_{n\geq 1}$ in $\mathcal{K}$, $(u_n(x))_{n\geq 1}$ is u.d. mod 1.

Σ^0_1-u.d. mod 1

Definition

A sequence $(x_n)_{n\geq 1}$ of reals is Σ^0_1-u.d. mod 1 if for every computably enumerable open set $A \subseteq [0,1]$,

$$\lim_{N\to\infty} \frac{1}{N} \# \Big\{ n : 1 \leq n \leq N, \{x_n\} \in A \Big\} = \mu(A).$$

Σ^0_1-u.d. mod 1 is different from u.d. mod 1

Proposition

If x is computable and irrational then $(nx)_{n\geq 1}$ is u.d. mod 1 but not Σ^0_1-u.d mod 1.

Σ_1^0-u.d. mod 1 is different from u.d. mod 1

Proposition

If x is computable and irrational then $(nx)_{n\geq 1}$ is u.d. mod 1 but not Σ_1^0-u.d mod 1.

Proof. Let x be computable and irrational, for example π.

$$A = \bigcup_{n\geq 1} \Big(\{nx\} - 2^{-n-3}\ ,\ \{nx\} + 2^{-n-3} \Big)$$

Then,

$$\mu(A) \leq \sum_{n\geq 1} 2\, 2^{-n-3} = 1/2 \quad \text{and} \quad \frac{1}{N}\#\Big\{ n : 1 \leq n \leq N, \{x_n\} \in A \Big\} = 1.$$

Hence, $(nx)_{n\geq 1}$ is not Σ_1^0-u.d. mod 1.

Almost all sequences are Σ_1^0-u.d. mod 1

Consider Lebesgue measure μ on $[0,1]$ and the product measure μ_∞ on $[0,1]^{\mathbb{N}}$.

Proposition (easy extension of Hlawka, 1956)

μ_∞-almost all elements in $[0,1]^{\mathbb{N}}$ are Σ_1^0-u.d. in the unit interval.

Inclusion

Theorem 3

Let x be a real number in $[0,1]$. If there is $(u_n : [0,1] \to \mathbb{R})_{n\geq 1}$ in $\mathcal{K}$ such that $(u_n(x))_{n\geq 1}$ is Σ^0_1-u.d. mod 1 then x is random.

Characterization

Theorem (Franklin, Greenberg, Miller, Ng 2012; Bienvenu, Day, Hoyrup, Mezhirov, Shen 2012)

A real x is random if and only if $(2^n x)$ is Σ^0_1-u.d. mod 1.

Randomness and uniform distribution

exists $(u_n)_{n\geq 1}$ in $\mathcal{K}$, $(u_n(x))_{n\geq 1}$ is Σ^0_1-u.d. mod 1

$\Downarrow \quad \Uparrow$?

$(2^n x)_{n\geq 1}$ is Σ^0_1-u.d. mod 1

$\Downarrow \quad \Uparrow$

x is random

$\Downarrow \quad \not\Uparrow$

for all $(u_n)_{n\geq 1}$ in $\mathcal{K}$ is $(u_n(x))_{n\geq 1}$ is u.d. mod 1

Discrepancy associated to random reals

Problem

Is there a random real x such that $(2^n x)_{n\geq 1}$ has discrepancy $O((\log N)/N)$?

Discrepancy associated random reals

Definition

$$D_N((x_n)_{n\geq 1}) = \sup_{0\leq u<v\leq 1} \left| \frac{\#\{n : 1 \leq n \leq N,\ u \leq \{x_n\} < v\}}{N} - (v-u) \right|$$

Discrepancy associated random reals

Definition

$$D_N((x_n)_{n\geq 1}) = \sup_{0\leq u<v\leq 1} \left| \frac{\#\{n : 1 \leq n \leq N,\ u \leq \{x_n\} < v\}}{N} - (v-u) \right|$$

Thus, $(x_n)_{n\geq 1}$ is u.d. mod 1 if $\lim_{N\to\infty} D_N((x_n)_{n\geq 1}) = 0$.

Discrepancy associated random reals

Definition

$$D_N((x_n)_{n\geq 1}) = \sup_{0\leq u<v\leq 1} \left| \frac{\#\{n : 1 \leq n \leq N,\ u \leq \{x_n\} < v\}}{N} - (v-u) \right|$$

Thus, $(x_n)_{n\geq 1}$ is u.d. mod 1 if $\lim_{N\to\infty} D_N((x_n)_{n\geq 1}) = 0$.

Schmidt, 1972, proved that there is a constant C such that for *every* $(x_n)_{n\geq 1}$ there are infinitely many Ns with

$$D_N((x_n)_{n\geq 1}) \geq C\frac{\log N}{N}.$$

There are Van der Corput sequences such that there is C such that for cofinitely many Ns,

$$D_N((x_n)_{n\geq 1}) \leq C\frac{\log N}{N}.$$

Selection that preserves uniform distribution modulo 1

Problem

What forms of selection of a subsequence preserve u.d. mod 1.

Selection that preserves uniform distribution modulo 1

In particular, $(2^n x)$ is u.d. mod 1 if and only if the selection by oblivious finite automaton of a sequence $(2^n x)$ is u.d. mod 1.

Selection that preserves uniform distribution modulo 1

In particular, $(2^n x)$ is u.d. mod 1 if and only if the selection by oblivious finite automaton of a sequence $(2^n x)$ is u.d. mod 1.

Let $x = a_1 a_2 \ldots$ be a word in alphabet A and let L be a regular language. The word obtained by prefix selection of x by L is $a_{k_1} a_{k_2} \ldots$, where $k_1 k_2 \ldots$ is the enumeration in increasing order of all the positive integers k such that $a_1 a_2 \ldots a_{k-1}$ is in L.

Theorem (Agafonov 1968)

Let L be a regular language and let x be a word in alphabet A. Then, if x is Borel normal then the word obtained by prefix selection of x by L is also Borel normal.

Selection that preserves uniform distribution modulo 1

In particular, $(2^n x)$ is u.d. mod 1 if and only if the selection by oblivious finite automaton of a sequence $(2^n x)$ is u.d. mod 1.

Let $x = a_1 a_2 \ldots$ be a word in alphabet A and let L be a regular language. The word obtained by prefix selection of x by L is $a_{k_1} a_{k_2} \ldots$, where $k_1 k_2 \ldots$ is the enumeration in increasing order of all the positive integers k such that $a_1 a_2 \ldots a_{k-1}$ is in L.

Theorem (Agafonov 1968)

Let L be a regular language and let x be a word in alphabet A. Then, if x is Borel normal then the word obtained by prefix selection of x by L is also Borel normal.

References

- J. Avigad. Uniform distribution and algorithmic randomness. *Journal of Symbolic Logic*, 78(1):334–344, 2013.
- Y. Bugeaud. *Distribution modulo one and Diophantine approximation*, volume 193 of *Cambridge Tracts in Mathematics*. Cambridge University Press, 2012.
- M. Drmota and R. Tichy. *Sequences, discrepancies and applications*. Lecture Notes in Mathematics. 1651. Springer, Berlin, 1997.
- J. F. Koksma. Ein mengentheoretischer satz über die gleichverteilung modulo eins. *Compositio Math*, 2:250–258, 1935.
- L. Kuipers and H. Niederreiter. *Uniform distribution of sequences*. Dover, 2006.
- W. Schmidt. Irregularities of distribution VII. *Acta Arithmetica*, 21:45–50, 1972.

Individual Ergodic Theorem

Let $(Y, \mathcal{F}, \nu)$, where ν is a non-negative normed measure, T is an ergodic transformation of Y with respect to ν and $\mathcal{F}$ is a σ-algebra. Then, for any ν-integrable function f on Y, for ν_∞ -almost every y in Y,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(T^n y) = \int_Y f \; d\nu.$$

Individual Ergodic Theorem

Let $(Y, \mathcal{F}, \nu)$, where ν is a non-negative normed measure, T is an ergodic transformation of Y with respect to ν and $\mathcal{F}$ is a σ-algebra. Then, for any ν-integrable function f on Y, for ν_∞ -almost every y in Y,

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} f(T^n y) = \int_Y f \ d\nu.$$

Let $Y = [0,1]^\infty$, T be the shift and let projection$p_1 : [0,1]^\infty \to [0,1]$, $p_1(x_1, x_2, \ldots) = x_1$. Then for any real valued Borel measurabe function f, for μ_∞ -almost every y,

$$\begin{aligned}
\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} f(x_n) &= \lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} f \circ p_1(T^n(x_1, x_2, \ldots)) \\
&= \int_{[0,1]^\infty} f \circ p_1 \ d\mu_\infty \\
&= \int_{[0,1]} f \ d\mu.
\end{aligned}$$