# Open questions
# on randomness and uniform distribution


Verónica Becher

Universidad de Buenos Aires


joint work with Serge Grigorieff and with Ted Slaman

Seminar on Computability Theory and Applications, March 9, 2021

# A wanted theorem

Computability theory has a notion of randomness for real numbers.

The theory of uniform distribution has a notion of equidistribution for sequences of real numbers.

## Wanted theorem

*A real number $x$ is random if and only if ... sequence associated to $x$ ... is uniformly distributed in the unit interval.*

# Randomness in computability theory

A real is random if it has no exceptional properties, if it avoids every effective $G_\delta$ null set.

## Definition (Martin-Löf randomness 1965)

*A real $x$ is random if for every uniformly computable sequence $(V_n)_{n\geq 1}$ of open sets of reals with Lebesegue measure $\mu(V_n) < 2^{-n}$,*

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

*Asking that $\mu(V)$ is computable, $x$ is Schnorr random.*

# Randomness in computability theory

The definition entails almost all (Lebesgue) real numbers are random.

Equivalent definition in terms of Kolmogorov complexity.

Examples: $\Omega$ numbers.

# Uniform distribution modulo one

## Definition

*A sequence of reals* $(x_n)_{n\geq 1}$ *is uniformly distributed modulo one, abbreviated u.d. mod* $1$*, if for every subinterval* $[a,b)$ *of the unit interval,*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \chi_{[a,b)}(\{x_n\}) = b - a$$

*where* $\{x\} = x - \lfloor x \rfloor = x \mod 1$

For example, convergent sequences are not u.d. mod $1$.

# u.d. mod 1

## Theorem

*Let* $(x_n)_{n\geq 1}$ *be a sequence of real numbers.*
*The following are equivalent:*

1. *The sequence* $(x_n)_{n\geq 1}$ *is u.d. mod* $1$.
2. *For every continuous* $f:\mathbb{R}\to\mathbb{C}$ *with period* $1$,

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

3. *Weyl's criterion: For every integer* $h$ *different from* $0$,

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

# u.d. mod 1

Consider Lebesgue measure $\mu$ on $[0, 1]$ and the product measure $\mu_\infty$ on $[0, 1]^{\mathbb{N}}$.

## Theorem (Hlawka, 1956)

*$\mu_\infty$-almost all sequences in $[0, 1]^{\mathbb{N}}$ are u.d. in the unit interval.*

# u.d. mod $1$

**Theorem** (Bohl; Sierpinski; 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 $1$.*

**Wanted theorem**

*A real $x$ is random if and only if $\ldots$ is u.d. mod $1$.*

# Koksma's General Metric Theorem

## Definition (Koksma 1935)

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

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

**Examples**

| | |
|---|---|
| $(x \mapsto nx)_{n\geq 1}$ | is in $\mathcal{K}$ |
| $(x \mapsto a_n x)_{n\geq 1}$ | is in $\mathcal{K}$, $(a_n)_{n\geq 1}$ of distinct integers |
| $(x \mapsto 2^n x)_{n\geq 1}$ | is in $\mathcal{K}$, |
| $(x \mapsto x^n)_{n\geq 1}$ | is not in $\mathcal{K}$. |
| $(x \mapsto x + na)_{n\geq 1}$ | is not in $\mathcal{K}$. |

# Koksma's General Metric Theorem

**Theorem** (Koksma General Metric Theorem 1935)

*Let $(u_n)_{n\geq 1}$ in $\mathcal{K}$. 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 $x$ is Schnorr random then for every computable $(a_n)_{n\geq 1}$ of distinct integers, $(a_n x)_{n\geq 1}$ is u.d. mod $1$.*

# Avigad's Theorem

**Theorem** (Avigad 2013)

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

**Definition**

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

**Theorem** (Becher and Grigorieff 2017)

*If $x$ in $[0,1]$ is Schnorr random then for every $(u_n)_{n\geq 1}$ in $\mathcal{K}^{\text{eff}}$, $(u_n(x))_{n\geq 1}$ is u.d. mod $1$.*

# The reverse of Avigad's theorem fails

**Theorem** (Algorithmic Randomness Workshop AIM, August 10-14, 2020)
*organized by Hirschfeldt, Miller, Reimann, and Slaman*

*There are non random reals, not even Kurtz random, such that for every computable $(a_n)_{n\geq 1}$ of distinct integers, $(a_n x)_{n\geq 1}$ is u.d. mod $1$.*

The counterexample constructed a $\Pi^0_1$ class of Fourier dimension $1$ but Lebesgue measure $0$.

**Conjecture** (Algorithmic Randomness Workshop AIM, August 10-14, 2020)

*If $x$ is random for a (computable) measure of positive Fourier dimension, then $(a_n x)_{n\geq 1}$ is u.d. mod $1$, for any computable sequence $(a_n)_{n\geq 1}$ of distinct integers.*

# $\Sigma_1^0$-u.d. mod 1

## Definition

*A sequence* $(x_n)_{n\geq 1}$ *of reals is* *$\Sigma_1^0$-u.d. mod 1* *if for every* $\Sigma_1^0$ *set* $A \subseteq [0,1]$

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \chi_A(\{x_n\}) = \mu(A),$$

*where* $\{x\} = x \mod 1 = x - \lfloor x \rfloor$.

## Proposition (easy extension of Hlawka, 1956)

$\mu_\infty$*-almost all sequences in* $[0,1]^{\mathbb{N}}$ *are* $\Sigma_1^0$*-u.d. in the unit interval.*

## Proposition

*If* $x$ *is computable and irrational then* $(nx)_{n\geq 1}$ *is u.d. mod* $1$ *but not* $\Sigma_1^0$*-u.d mod* $1$.

# Randomness and $\Sigma^0_1$-u.d. $\mod 1$

Theorem (Becher and Grigorieff 2017)

*Let $x$ in $[0,1]$. If $(u_n)_{n\geq 1}$ in $\mathcal{K}^{eff}$ and $(u_n(x))_{n\geq 1}$ is $\Sigma^0_1$-u.d. mod $1$ then $x$ is random.*

# Randomness and $\Sigma^0_1$-u.d. $\mod 1$

**Theorem** (Becher and Grigorieff 2017)

*Let $x$ in $[0,1]$. If $(u_n)_{n\geq 1}$ in $\mathcal{K}^{\mathit{eff}}$ and $(u_n(x))_{n\geq 1}$ is $\Sigma^0_1$-u.d. mod $1$ then $x$ is random.*

The next follows from the characterization of randomness in terms of effective version of Birkhoff's ergodic theorem,

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

*A real $x$ is random if and only if $(2^n x)_{n\geq 1}$ is $\Sigma^0_1$-u.d. mod $1$.*

# An effective version of Birkhoff's ergodic theorem

## Theorem (Franklin, Greenberg, Miller and Ng 2012 Theorem 6 )

*Bienvenu,Day,Hoyrup,Mezhirov and Shen 2012 Theorem 8 proved the left to right implications.*

*Let $(X, \mu)$ be a computable probability space and let $T : X \to X$ be a computable ergodic map. A point $x \in X$ is random if and only if for every effectively closed subset $U$ of $X$,*

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N-1} \chi_U(T^n(x)) = \mu(U).$$

## Corollary

*Let $T : X \to X$ be a computable ergodic map.*
*A point $x$ is random if and only if $(T^n x)_{n \geq 1}$ is $\Sigma_1^0$-u.d. mod $1$.*

In particular, $(2^n x)_{n \geq 1}$.

# Iterations on ergodic maps and $\mathcal{K}$ do not coincide

**Observation**

$T : x \mapsto 2x \pmod 1$ on $[0, 1]$ is ergodic and $(x \mapsto 2^n x)_{n\geq 0}$ is in $\mathcal{K}^{\text{eff}}$

$T : x \mapsto x + a \pmod 1$ on $[0, 1]$ is ergodic when $a$ is irrational but $(x \mapsto x + na)_{n\geq 0}$ is not in $\mathcal{K}^{\text{eff}}$.

# Separations on randomness and uniform distribution

## Question 1

*for all* $(u_n)_{n\geq 1}$ *in* $\mathcal{K}^{\text{eff}}$, $(u_n(x))_{n\geq 1}$ *is* $\Sigma^0_1$*-u.d. mod* $1$

$\Downarrow \quad \Uparrow ?$

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

$\Downarrow ? \quad \Uparrow$

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

$\Downarrow \quad \Uparrow$

$x$ *is random*

$\Downarrow \quad \not\Uparrow$

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

$\Downarrow \quad \not\Uparrow ?$

*for all* $(a_n)_{n\geq 1}$ *distinct integers,* $(a_n(x))_{n\geq 1}$ *is u.d. mod* $1$

# Discrepancy of sequences of reals

## Definition

*For $(x_n)_{n\geq 1}$ of reals in $[0,1)$ the discrepancy of the $N$ first elements is*

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

# Discrepancy of sequences of reals

## Definition

*For* $(x_n)_{n\geq 1}$ *of reals in* $[0,1)$ *the discrepancy of the* $N$ *first elements is*

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

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 of sequences of reals

**Theorem** (Schmidt, 1972)

*There is a constant $C$ such that for every $(x_n)_{n\geq 1}$ there are infinitely many $N$s with*

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

This lower bound is achieved by van der Corput sequences.

# Discrepancy associated to real numbers

**Theorem** (M. Levin 1999; Becher and Carton 2019)

*There is a computable real $x$ and a constant $c$ such that for all $N$, $D_N((2^n x)_{n\geq 0}) \leq c\frac{\log^2 N}{N}$.*

**Theorem** (Aistleitner, Becher, Scheerer and Slaman 2017)

*There is a computable real $x$ such that for each $b \geq 2$, there are numbers $N_0$ and $C$ such that for all $N \geq N_0$, $D_N((b^n x)_{n\geq 0}) \leq \frac{C}{\sqrt{N}}$.*

# Discrepancy associated to random real numbers

**Theorem** (Gál and Gál 1964; Philipp 1975; Fukuyama 2008)

*There is a constant $c$ such that for almost all (Lebesgue measure) reals, for cofinitely many $N$s,*

$$D_N((2^n x)_{n\geq 1}) \leq c\sqrt{\frac{\log\log N}{N}}$$

*and this upper bound is reached for infinitely many $N$s.*

**Question 2**

*What is the minimal discrepancy $D_N((2^n x)_{n\geq 1})$ for a random real $x$?*

# Randomness with respect to Fourier measures

## Theorem (Slaman 2019)

*If a real is random with respect to a non-trivial Fourier measure then for all integers $b \geq 2$, $(b^n x)_{n \geq 1}$ is u.d. mod $1$, and there is a linear lower bound on its Kolmogorov complexity.*

## Question 3

*If a real is random with respect to a non-trivial Fourier measure, what is the discrepancy $D_N((b^n x)_{n \geq 1})$ for each integer $b \geq 2$?*

# Poisson generic reals

Convergence to the Poisson law. Suppose an event $X$ has probability $p$. The probability of exactly $k$ occurrences of $X$ in $N$ independent draws is

$$\binom{N}{k} p^k (1-p)^{N-k}$$

Let $\lambda > 0$ and for each $N$ let $p = \lambda/N$. So, for each fixed integer $k \geq 0$,

$$\lim_{\substack{N\to\infty \\ p=\lambda/N}} \binom{N}{k} p^k (1-p)^{N-k} = \lim_{N\to\infty} \binom{N}{k} \left(\frac{\lambda}{N}\right)^k \left(1-\frac{\lambda}{N}\right)^{N-k}$$

$$= \lim_{N\to\infty} \frac{N(N-1)\cdots(N-k+1)}{N^k} \left(1-\frac{\lambda}{N}\right)^N \frac{\lambda^k}{k!}$$

$$= e^{-\lambda}\frac{\lambda^k}{k!}$$

and it holds that $\sum_{k\geq 0} e^{-\lambda}\frac{\lambda^k}{k!} = 1$.

# Poisson generic reals

The initial segment of length $N = \lfloor \lambda 2^n \rfloor$ of a sequence is $N$ independent draws of length-$n$ words, thus $p = \lambda / N = \lambda / \lfloor \lambda 2^n \rfloor$

## Definition

*A binary sequence $x$ is Poisson generic if for all $\lambda > 0$ and all integer $k \geq 0$,*

$$\lim_{n\to\infty} \frac{\#\text{ length-}n\text{ words occur exactly }k\text{ times in first }\lfloor \lambda 2^n \rfloor\text{ symbols of }x}{\#\text{ length-}n\text{ words}} = e^{-\lambda}\frac{\lambda^k}{k!}.$$

# Poisson generic reals

### Theorem (Peres and Weiss)

*Almost all (Lebesgue measure) real numbers are Poisson generic.*

### Theorem (Peres and Weiss)

*Poisson generic reals are Borel normal.*

Champernowne sequence is not Poisson generic. No examples are known.

### Question 4

*Is there a computable Poisson generic real?*

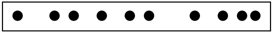
Analog to the work started with Turing 1937, incrementally construct initial segment that avoids a null set.

### Question 5

*Are all random real numbers Poisson generic?*

# Poissonian pair correlations

A sequence $(x_n)_{n\geq 1}$ of reals in $[0,1]$ has Poissonian pair correlation if for all $s>0$ for every positive $s$, in the limit, in the first $N$ elements, the proportion of pairs at distance less than $s/N$ is $2s$.



Divide the unit interval in $N$ pieces, take $s=1$, then the property asks that each bullet has one neighbour at the left and one neighbour at the right at distance less than $1/N$.

# Poissonian pair correlation

## Definition

*A sequence* $(x_n)_{n\geq 1}$ *has Poissonian pair correlations if for all* $s > 0$*,*

$$\lim_{N\to\infty} F_N(s) = 2s,$$

*where*

$$F_N(s) = \frac{1}{N}\#\left\{ (i,j) \,:\, 1 \leq i \neq j \leq N \text{ and } \|x_i - x_j\| < \frac{s}{N} \right\}.$$

*and* $\|x\|$ *is the distance from* $x$ *to the nearest integer.*

# Poissonian pair correlation

Theorem (Grepstad and G.Larcher 2017; Aistleitner, Lachmann and Pausinger 2018)

*Poissonian pair correlation implies equidistribution.*

Proposition

$\mu_\infty$*-almost all sequences in* $[0,1]^{\mathbb{N}}$ *have Poissonian pair correlation.*

# Real numbers and Poissonian pair correlation

The following have Poissonian pair correlation:

- $(\{\sqrt{n}\})_{n\geq 1}$ (El Baz, Marklof and Vinogradov 2015)
- $(\{n^d x\})_{n\geq 0}$ for $d \geq 2$ for almost all $x$ (Rudnick and Sarnak, 1997)
- $(\{2^n x\})_{n\geq 0}$ for almost all $x$ (Rudnick and Zaharescu 2002)

The following fail Poissonian pair correlation:

- The Kronecker sequence $(\{nx\})_{n\geq 1}$, for every real $x$
- many known constructed constants,
  (Pirsic and Stockinger, 2018;Becher, Carton and Mollo Cunnigham 2019)

# Real numbers and Poissonian pair correlation

## Question 6

*Is there a computable $x$ such that $(\{2^n x\})_{n\geq 1}$ has Poissonian pair correlation?*

## Question 7

*For all random reals $x$, $(\{2^n x\})_{n\geq 1}$ has Poissonian pair correlation?*

# Descriptive complexity in the Arithmetical Hierarchy

## Theorem

- *The set of Borel normal to base $2$ is $\Pi^0_3$ complete,* *Ki and Linton 1994*
- *The set of Borel normal to every base numbers is $\Pi^0_3$ complete,* *Becher, Heiber and Slaman 2014*
- *The set of numbers that are normal to some base is $\Sigma^0_4$ complete,* *Becher and Slaman 2016*
- *The set of bases for which a real number is simply normal depends just on multiplicative dependence, no logical tights,* *Becher, Bugeaud and Slaman 2016*
- *The set of reals $x$ for which there is a Fourier measure that makes $x$ random is $\Sigma^0_2$ complete,* *Marcone, Reimann, Slaman and Valenti 2020*
- *Normal numbers to base $b$ that preserve normality under addition is $\Pi^0_3$-complete,* *Airey, Jackson and Mance 2020*
- *Borel complexity of sets of normal numbers in several numeration systems,* *Airey, Jackson, Kwietniak and Mance 2020*

# Descriptive Complexity in the Arithmetical Hierarchy

## Question 8

*Prove that the set of Poisson generic real numbers is* $\Pi^0_3$*-complete.*

## Question 9

*Prove that the set of reals* $x$ *such that* $(\{2^n x\})_{n\geq 1}$ *has Poissonian pair correlation is* $\Pi^0_3$*-complete.*

# Summary of the open questions

**Random reals and u.d.**

- $(2^n x)_{n\geq1}$ versus $(u_n(x))_{n\geq1}$ for $(u_n)$ in $\mathcal{K}^{\text{eff}}$
- Conjecture: If $x$ is random for a measure of positive Fourier dimension then $(a_n x)_{n\geq1}$ is u.d. mod $1$, when $(a_n)_{n\geq1}$ is sequence of distict integers.
- For all $x$ random is $x$ Poisson generic?
- For all $x$ random, has $(\{2^n x\})_{n\geq1}$ Poissonian pair correlation?

**Is there a computable real $x$ such that**

- $x$ that is Poission generic?
- $(\{2^n x\})_{n\geq1}$ has Poissonian pair correlation?

**Discrepancy**

- What is the minimal discrepancy of $D_N((2^n x)_{n\geq1})$ for all random $x$?
- What is the discrepancy of $D_N((b^n x))_{n\geq1}$ for $x$ random with respect to a Fourier measure?

**Descriptive complexity of the mentioned properties?**

- C. Aistleitner, V. Becher, A.-M. Scheerer and T. Slaman. On the construction of absolutely normal numbers, *Acta Arithmetica* 180(4): 333–346, 2017.
- J. Avigad. Uniform distribution and algorithmic randomness. *Journal of Symbolic Logic*, 78(1):334–344, 2013.
- V. Becher and S. Grigorieff. Randomness and uniform distribution, manuscript 2017.
- L. Bienvenu, A. Day, M. Hoyrup, Mezhirov and A. Shen. A constructive version of Birkhoff's ergodic theorem for Martin-Lf random points. *Information and Computation* 210 : 2130, 2012.
- J. Franklin, N. Greenbergm, J. S. Miller and K.M. Ng. Martin-Löf random points satisfy Birkhoff ergodic theorem for effectively closed sets. *Proceedings of the American Mathematical Society* 140(10):3623–3628, 2012.
- 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.
- I.S Gál and L. Gál. The discrepancy of the sequence $(2^n x)$. *Indag. Math* 26: 129-143, 1964.
- 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.
- M. B. Levin. On the discrepancy estimate of normal numbers. *Acta Arithmetica* 88(2):99–111, 1999.
- W. Schmidt. Irregularities of distribution VII. *Acta Arithmetica*, 21:45–50, 1972.
- C. Aistleitner and T. Lachmann and F. Pausinger. Pair correlations and equidistribution, *Journal of Number Theory*, 182:206–220, 2018.
- V. Becher and O. Carton and I. Mollo. Low discrepancy sequences failing Poissonian pair correlations. *Archiv der Mathematik* 113(2):169178,2019.
- D. El-Baz and J. Marklof and I. Vinogradov. The two-point correlation function of the fractional parts of $\sqrt{n}$ is Poisson, *Proceedings of the American Mathematical Society*, 143(7): 2815–2828, 2015.
- Í. Pirsic and W. Stockinger. The Champernowne constant is not Poissonian. *Functiones et Approximatio Commentarii Mathematici* 60(2):253–262, 2019.
- Z. Rudnick and A. Zaharescu. *A metric result on the pair correlation of fractional parts of sequences*. Acta Arithmetica 89:283–293, 1999.

## Theorem (Bienvenu, Day, Hoyrup, Mezhirov and Shen 2012 Theorem 8)

*Let $\mu$ a computable measure on $X$. Let $T : X \to X$ be a computable almost everywhere defined $\mu$-preserving ergodic transformation. Let $U$ be an effectively open set. For every Martin-Löf random point $x$,*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n-1} \chi_U(T^k(x)) = \mu(U)$$

## Theorem (Franklin, Greenberg, Miller and Ng 2012 Theorem 6 )

*Let $X$ be a computable probability space and let $T : X \to X$ be a computable ergodic map. Then, $x \in X$ is Martin-Löf random if and only if for all effectively closed $U$ included in $X$*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n-1} \chi_U(T^k(x)) = \mu(U)$$