Random Functions

Jan Reimann

Institut für Informatik, Universität Heidelberg

Random reals and random sequences

- When we speak of random reals, we usually mean a random infinite binary sequence (which represents a real).

Random reals and random sequences

- When we speak of random reals, we usually mean a random infinite binary sequence (which represents a real).
- Justification: randomness is base invariant. The g-ary expansion of a real number is ML-random iff the h-ary is ($g, h \geq 2$).

Random reals and random sequences

- When we speak of random reals, we usually mean a random infinite binary sequence (which represents a real).
- Justification: randomness is base invariant. The g-ary expansion of a real number is ML-random iff the h-ary is ($g, h \geq 2$).
- This invariance constrasts normality, which is not base-independent. (Cassels, 1959).

Random reals and random sequences

- When we speak of random reals, we usually mean a random infinite binary sequence (which represents a real).
- Justification: randomness is base invariant. The g-ary expansion of a real number is ML-random iff the h-ary is ($g, h \geq 2$).
- This invariance constrasts normality, which is not base-independent. (Cassels, 1959).
- Base-invariance of randomness has been proved by a number of people: Calude and Jürgensen (1994), Staiger (1998), Hertling and Weihrauch (1998).

Conservation of randomness

- Base-invariance is already implicit in a fundamental result by Levin (1974): Conservation of randomness.

Conservation of randomness

- Base-invariance is already implicit in a fundamental result by Levin (1974): Conservation of randomness.
- Let μ be a measure on 2^ω, $\Phi : 2^\omega \to 2^\omega$ a transformation. This induces an image measure μ_Φ:

$$\mu_\Phi[\sigma] = \mu\Phi^{-1}[\sigma]$$

Conservation of randomness

- Base-invariance is already implicit in a fundamental result by Levin (1974): Conservation of randomness.
- Let μ be a measure on 2^ω, $\Phi : 2^\omega \to 2^\omega$ a transformation. This induces an image measure μ_Φ:

$$\mu_\Phi[\sigma] = \mu\Phi^{-1}[\sigma]$$

- Theorem: [Levin] If Φ is computable and ξ is μ-random, then $\Phi\xi$ is μ_Φ-random.

Continued fractions

- There is another important representation of reals: The continued fraction expansion.

Continued fractions

- There is another important representation of reals: The continued fraction expansion.
- For $\alpha \in \mathbb{R}$, let $[\alpha]$ denote the integral part, and $\{\alpha\}$ denote the non-integral part of α, so $\alpha = [\alpha] + \{\alpha\}$, $[\alpha] \in \mathbb{Z}$, $\{\alpha\} \in [0, 1)$.

Continued fractions

- There is another important representation of reals: The continued fraction expansion.
- For $\alpha \in \mathbb{R}$, let $[\alpha]$ denote the integral part, and $\{\alpha\}$ denote the non-integral part of α, so $\alpha = [\alpha] + \{\alpha\}$, $[\alpha] \in \mathbb{Z}$, $\{\alpha\} \in [0,1)$.
- Given α, set $\alpha_0 = \alpha$ and let, for $n \geq 0$,

$$a_n = [\alpha_n] \quad \text{and} \quad \alpha_{n+1} = \frac{1}{\{\alpha_n\}}.$$

(Stop if $\{\alpha_n\} = 0$.)

Continued fractions

- There is another important representation of reals: The continued fraction expansion.
- For $\alpha \in \mathbb{R}$, let $[\alpha]$ denote the integral part, and $\{\alpha\}$ denote the non-integral part of α, so $\alpha = [\alpha] + \{\alpha\}$, $[\alpha] \in \mathbb{Z}$, $\{\alpha\} \in [0, 1)$.
- Given α, set $\alpha_0 = \alpha$ and let, for $n \geq 0$,

$$a_n = [\alpha_n] \quad \text{and} \quad \alpha_{n+1} = \frac{1}{\{\alpha_n\}}.$$

  (Stop if $\{\alpha_n\} = 0$.)
- The process is finite iff α is rational.

The continued fraction expansion

- For irrational numbers, the partial convergents

$$[a_0, a_1, \ldots a_n] := \frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots \frac{1}{a_n}}}} \qquad a_i \in \mathbb{N}$$

converge to α.

The continued fraction expansion

- For irrational numbers, the partial convergents

$$[a_0, a_1, \ldots a_n] := \frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots \frac{1}{a_n}}}} \qquad a_i \in \mathbb{N}$$

converge to α.

- The continued fraction expansion induces a bijection between the irrational reals and the set of all infinite sequences of natural numbers, the Baire space $\mathbb{N}^{\mathbb{N}}$.

A few examples

- Continued fractions are extremely important in number theory. (We will see later why.)

A few examples

- Continued fractions are extremely important in number theory. (We will see later why.)
- Golden mean $(1 + \sqrt{5})/2 = [1, 1, 1, 1, \ldots]$.

A few examples

- Continued fractions are extremely important in number theory. (We will see later why.)
- Golden mean $(1+\sqrt{5})/2 = [1, 1, 1, 1, \ldots]$.
- $\sqrt{2}/2 = [1, 2, 2, 2, \ldots]$.

A few examples

- Continued fractions are extremely important in number theory. (We will see later why.)
- Golden mean $(1+\sqrt{5})/2 = [1, 1, 1, 1, \ldots]$.
- $\sqrt{2}/2 = [1, 2, 2, 2, \ldots]$.
- $e \mod 1 = [1, 2, 1, 1, 4, 1, 1, 6, \ldots]$.

A few examples

- Continued fractions are extremely important in number theory. (We will see later why.)
- Golden mean $(1+\sqrt{5})/2 = [1, 1, 1, 1, \dots]$.
- $\sqrt{2}/2 = [1, 2, 2, 2, \dots]$.
- $e \mod 1 = [1, 2, 1, 1, 4, 1, 1, 6, \dots]$.
- $\pi \mod 1 = [7, 15, 1, 292, 1, 1, \dots]$.

Random continued fractions

- As the transformation is effective, we would expect invariance to hold for continued fractions (cf), too.

Random continued fractions

- As the transformation is effective, we would expect invariance to hold for continued fractions (cf), too.
- But: what is a random continued fraction?

Random continued fractions

- As the transformation is effective, we would expect invariance to hold for continued fractions (cf), too.
- But: what is a random continued fraction?
- One can think of two possibilities to define this:

Random continued fractions

- As the transformation is effective, we would expect invariance to hold for continued fractions (cf), too.
- But: what is a random continued fraction?
- One can think of two possibilities to define this:
  - Say a cf is random if the sequence obtained by the binary expansion of the accordant real is random.

The ‘randomness machinery’

- Measure theoretic [Martin-Löf]:
  A sequence is random if it is not an effective nullset.

The ‘randomness machinery’

- Measure theoretic [Martin-Löf]:
  A sequence is random if it is not an effective nullset.
- Information theoretic [Kolmogorov; Levin; Chaitin]
  A sequence is random if it is incompressible.

The 'randomness machinery'

- Measure theoretic [Martin-Löf]:
  A sequence is random if it is not an effective nullset.
- Information theoretic [Kolmogorov; Levin; Chaitin]
  A sequence is random if it is incompressible.
- Schnorr's Theorem: Both approaches yield the same concept.

The ‘randomness machinery’

- Measure theoretic [Martin-Löf]:
  A sequence is random if it is not an effective nullset.
- Information theoretic [Kolmogorov; Levin; Chaitin]
  A sequence is random if it is incompressible.
- Schnorr’s Theorem: Both approaches yield the same concept.
- Key ingredient to the proof: Coding Theorem [Zvonkin-Levin].

Measure on Baire Space

- Basic open cylinders: convergents of continued fractions, $[a_0, \ldots a_n]$.

Measure on Baire Space

- Basic open cylinders: convergents of continued fractions, $[a_0, \dots a_n]$.
- In the following, identify an initial segment $[a_1, \dots, a_n]$ of a continued fraction with the n-convergent

$$\frac{p_n}{q_n} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots \cfrac{1}{a_n}}}}.$$

Measure on Baire Space

- Basic open cylinders: convergents of continued fractions, $[a_0, \ldots a_n]$.
- In the following, identify an initial segment $[a_1, \ldots, a_n]$ of a continued fraction with the n-convergent

$$\frac{p_n}{q_n} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots \cfrac{1}{a_n}}}}.$$

- The diameter of a cylinder (as a subset of $[0, 1]$) is:

$$\operatorname{diam}[a_0, \ldots a_n] = \frac{1}{q_n(q_n + q_{n-1})}$$

Effective measure

- A set $\mathcal{A} \subseteq \mathbb{N}^{\mathbb{N}}$ is effectively null, if there is a recursive sequence (C_n) of r.e. sets such that for each n,

$$\mathcal{A} \subseteq \bigcup_{w \in C_n} [w] \quad \text{and} \quad \sum_{w \in C_n} \mathrm{diam}[w] \leq 2^{-n}.$$

Effective measure

- A set $\mathcal{A} \subseteq \mathbb{N}^{\mathbb{N}}$ is effectively null, if there is a recursive sequence (C_n) of r.e. sets such that for each n,

$$\mathcal{A} \subseteq \bigcup_{w \in C_n} [w] \quad \text{and} \quad \sum_{w \in C_n} \mathrm{diam}[w] \leq 2^{-n}.$$

- A cf α is random if $\{\alpha\} \subseteq \mathbb{N}^{\mathbb{N}}$ is not effectively null.

Random Continued Fractions

- Initial question: Is randomness invariant with respect to different representations (g-adic, continued fraction) of a real?

Random Continued Fractions

- Initial question: Is randomness invariant with respect to different representations (g-adic, continued fraction) of a real?
- Problem: The continued fraction expansion might code things more efficiently.

Comparing expansions

- Let θ be irrational. Suppose $\mathrm{E}_2(\theta)\restriction_n = \theta_1\theta_2\ldots\theta_n$ are the first n digits of its binary expansion. Set

$$r_n = r_n(\theta) = \sum_{i=1}^{n} \theta_i 2^{-i} \quad \text{and} \quad s_n = s_n(\theta) = \sum_{i=1}^{n} \theta_i 2^{-i} + \frac{1}{2^n}.$$

Comparing expansions

- Let θ be irrational. Suppose $\mathrm{E}_2(\theta)\restriction_n = \theta_1\theta_2\ldots\theta_n$ are the first n digits of its binary expansion. Set

$$r_n = r_n(\theta) = \sum_{i=1}^{n} \theta_i 2^{-i} \quad \text{and} \quad s_n = s_n(\theta) = \sum_{i=1}^{n} \theta_i 2^{-i} + \frac{1}{2^n}.$$

- r_n and s_n are rational, hence their continued fraction expansions finite. Assume

$$\mathrm{CF}(r_n) = [a_1, a_2, \ldots, a_k] \text{ and } \mathrm{CF}(s_n) = [b_1, b_2, \ldots, b_l].$$

Comparing expansions

- Let θ be irrational. Suppose $\mathrm{E}_2(\theta)\restriction_n = \theta_1\theta_2\ldots\theta_n$ are the first n digits of its binary expansion. Set

$$r_n = r_n(\theta) = \sum_{i=1}^{n} \theta_i 2^{-i} \quad \text{and} \quad s_n = s_n(\theta) = \sum_{i=1}^{n} \theta_i 2^{-i} + \frac{1}{2^n}.$$

- r_n and s_n are rational, hence their continued fraction expansions finite. Assume

$$\mathrm{CF}(r_n) = [a_1, a_2, \ldots, a_k] \text{ and } \mathrm{CF}(s_n) = [b_1, b_2, \ldots, b_l].$$

- Let $N = \max\{j : \ a_j = b_j\}$ and set $\pi_n(\theta) = [a_1, \ldots, a_N]$.

Comparing expansions

- We cannot simply convert $\mathrm{E}_2(\theta)\restriction_n$ into a continued fraction.

Comparing expansions

- We cannot simply convert $\mathrm{E}_2(\theta)\restriction_n$ into a continued fraction.
- Let $\theta = \sqrt[3]{2} - 1 = 0.259921\ldots$ (decimal expansion). We have

$$r_5 = 0.25992 \quad \text{and} \quad s_5 = 0.25993.$$

Comparing expansions

- We cannot simply convert $\mathrm{E}_2(\theta)\restriction_n$ into a continued fraction.
- Let $\theta = \sqrt[3]{2} - 1 = 0.259921\ldots$ (decimal expansion). We have

$$r_5 = 0.25992 \quad \text{and} \quad s_5 = 0.25993.$$

- The continued fraction algorithm yields

$$\begin{aligned} \mathrm{CF}(r_5) &= [3,1,5,1,1,4,2,5,1,3] \\ \mathrm{CF}(s_5) &= [3,1,5,1,1,5,5,1,2,1,4,3]. \end{aligned}$$

Therefore $\pi_5(\theta) = [3,1,5,1,1]$.

Comparing expansions

- Question: How does $|\pi_n(\xi)|$ relate to n?

Comparing expansions

- Question: How does $|\pi_n(\xi)|$ relate to n?
- Theorem: [Lochs] For almost every $\xi \in 2^\omega$,

$$\lim_{n\to\infty} \frac{|\pi_n(\xi)|}{n} = \frac{6\log^2 2}{\pi^2}.$$

Comparing expansions

- Question: How does $|\pi_n(\xi)|$ relate to n?
- Theorem: [Lochs] For almost every $\xi \in 2^\omega$,

$$\lim_{n\to\infty} \frac{|\pi_n(\xi)|}{n} = \frac{6\log^2 2}{\pi^2}.$$

- At the heart of Lochs' result lies a fundamental fact about the asymptotic behaviour of the partial convergents.

Comparing expansions

- Question: How does $|\pi_n(\xi)|$ relate to n?
- Theorem: [Lochs] For almost every $\xi \in 2^\omega$,

$$\lim_{n\to\infty} \frac{|\pi_n(\xi)|}{n} = \frac{6\log^2 2}{\pi^2}.$$

- At the heart of Lochs' result lies a fundamental fact about the asymptotic behaviour of the partial convergents.
- Theorem: [Khintchine] For almost every $\alpha \in \mathbb{R}$,

$$\frac{1}{n}\log q_n(\alpha) \longrightarrow \frac{\pi^2}{12\log 2}.$$

Digression: Ergodic Theorem

- Let (X, μ) be some measure space (Borel), $T : X \to X$ μ-preserving, that is, $\mu A = \mu T^{-1} A$ for all A Borel. T is ergodic if $TA = A$ implies $\mu A \in \{0, 1\}$.

Digression: Ergodic Theorem

- Let (X, μ) be some measure space (Borel), $T : X \to X$ μ-preserving, that is, $\mu A = \mu T^{-1} A$ for all A Borel. T is ergodic if $TA = A$ implies $\mu A \in \{0, 1\}$.
- Theorem: [Birkhoff] For any continous $f : X \to \mathbb{R}$, ergodic T, and μ-almost every $x \in X$, it holds that

$$\frac{1}{n} \sum_{i=0}^{n-1} f(T^i x) \longrightarrow \int f d\mu.$$

Digression: Ergodic Theorem

- Let (X, μ) be some measure space (Borel), $T : X \to X$ μ-preserving, that is, $\mu A = \mu T^{-1} A$ for all A Borel. T is ergodic if $TA = A$ implies $\mu A \in \{0, 1\}$.
- Theorem: [Birkhoff] For any continous $f : X \to \mathbb{R}$, ergodic T, and μ-almost every $x \in X$, it holds that

$$\frac{1}{n} \sum_{i=0}^{n-1} f(T^i x) \longrightarrow \int f d\mu.$$

- Gauss map $x \mapsto \frac{1}{x} \mod 1$ describes the shift map for continued fractions. Its entropy is $\pi^2/6 \log 2$.

Digression: Ergodic Theorem

- Let (X, μ) be some measure space (Borel), $T : X \to X$ μ-preserving, that is, $\mu A = \mu T^{-1} A$ for all A Borel. T is ergodic if $TA = A$ implies $\mu A \in \{0, 1\}$.
- Theorem: [Birkhoff] For any continous $f : X \to \mathbb{R}$, ergodic T, and μ-almost every $x \in X$, it holds that

$$\frac{1}{n} \sum_{i=0}^{n-1} f(T^i x) \longrightarrow \int f d\mu.$$

- Gauss map $x \mapsto \frac{1}{x} \mod 1$ describes the shift map for continued fractions. Its entropy is $\pi^2 / 6 \log 2$.
- However, the ergodic theorem is not effective (Vyugin, 1998).

Proving Invariance

- Theorem: The set of irrational numbers θ that do not satisfy Lochs' theorem is an effective nullset.

Proving Invariance

- Theorem: The set of irrational numbers θ that do not satisfy Lochs' theorem is an effective nullset.
- Theorem: [Faivre] For all $\varepsilon > 0$, there exist positive constants c, δ (depending on ε) with $0 < \delta < 1$ such that

$$\lambda\left(\left\{\xi \in \mathbb{R} : \left|\frac{|\pi_n \theta|}{n} - L\right| \geq \varepsilon\right\}\right) \leq c\delta^n$$

for all integers $n \geq 1$ and with $L = 6\log^2 2/\pi^2$.

Proving Invariance

- Theorem: The set of irrational numbers θ that do not satisfy Lochs' theorem is an effective nullset.
- Theorem: [Faivre] For all $\varepsilon > 0$, there exist positive constants c, δ (depending on ε) with $0 < \delta < 1$ such that

$$\lambda\left(\left\{\xi \in \mathbb{R} : \left|\frac{|\pi_n\theta|}{n} - L\right| \geq \varepsilon\right\}\right) \leq c\delta^n$$

  for all integers $n \geq 1$ and with $L = 6\log^2 2/\pi^2$.
- Result is based on transfer operators (Mayer, Ruelle).

Properties of random continued fractions

- The use of transfer operators allows to effectivize a lot of results on continued fractions.

Properties of random continued fractions

- The use of transfer operators allows to effectivize a lot of results on continued fractions.
- Theorem: A random cf must have arbitrary large partial quotients, i.e. the numbers occuring in a typical cf are unbounded.

Properties of random continued fractions

- The use of transfer operators allows to effectivize a lot of results on continued fractions.
- Theorem: A random cf must have arbitrary large partial quotients, i.e. the numbers occuring in a typical cf are unbounded.
- Theorem: An irrational α is badly approximable if and only if its continued fraction expansion is bounded.

Diophantine Approximation

- Diophantine Approximation classifies real numbers by how well they may be approximated by rational numbers.

Diophantine Approximation

- Diophantine Approximation classifies real numbers by how well they may be approximated by rational numbers.
- Fundamental Theorem of Dirichlet: For any irrational α there exist infinitely many p/q (rel. prime) such that

$$|\alpha - p/q| \leq 1/q^2.$$

Diophantine Approximation

- Diophantine Approximation classifies real numbers by how well they may be approximated by rational numbers.
- Fundamental Theorem of Dirichlet: For any irrational α there exist infinitely many p/q (rel. prime) such that

$$|\alpha - p/q| \leq 1/q^2.$$

- A sequence of infinitely many such fractions is given by the partial convergents of the continued fraction expansion of α.

Diophantine Approximation

- In general, one cannot improve the factor 2 in Dirichlet's theorem.

Diophantine Approximation

- In general, one cannot improve the factor 2 in Dirichlet's theorem.
- A number β is badly approximable if there exists a K such that

$$\forall p/q \in \mathbb{Q}\ |\beta - p/q| \geq K/q^2.$$

Diophantine Approximation

- In general, one cannot improve the factor 2 in Dirichlet's theorem.
- A number β is badly approximable if there exists a K such that

$$\forall p/q \in \mathbb{Q}\ |\beta - p/q| \geq K/q^2.$$

- Examples:

Diophantine Approximation

- Algebraic numbers are close to badly approximable:

Diophantine Approximation

- Algebraic numbers are close to badly approximable:
- Roth's Theorem: For any algebraic α, for any $\varepsilon > 0$,

$$|\alpha - \frac{p}{q}| \leq \frac{1}{q^{2+\varepsilon}} \qquad \text{(-1)}$$

has only finitely many solutions.

Properties of random continued fractions

- The use of transfer operators allows to effectivize a lot of results on continued fractions.

Properties of random continued fractions

- The use of transfer operators allows to effectivize a lot of results on continued fractions.
- Theorem: A random cf must have arbitrary large partial quotients, i.e. the numbers occuring in a typical cf are unbounded.

Properties of random continued fractions

- The use of transfer operators allows to effectivize a lot of results on continued fractions.
- Theorem: A random cf must have arbitrary large partial quotients, i.e. the numbers occuring in a typical cf are unbounded.
- Theorem: An irrational α is badly approximable if and only if its continued fraction expansion is bounded.

Properties of random continued fractions

- On the other hand, random reals cannot be too well-approximable.

Properties of random continued fractions

- On the other hand, random reals cannot be too well-approximable.
- A Liouville number is an irrational α for which

$$(\forall n)\,(\exists p,q)\,\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^n}.$$

Example: $\sum 10^{-n!}$.

Properties of random continued fractions

- On the other hand, random reals cannot be too well-approximable.
- A Liouville number is an irrational α for which

$$(\forall n)\,(\exists p, q)\,\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^n}.$$

Example: $\sum 10^{-n!}$.

- Theorem: [Staiger] No Liouville number is a random real.

Properties of random continued fractions

- It turns out that random reals must be close to badly approximable.

Properties of random continued fractions

- It turns out that random reals must be close to badly approximable.
- Theorem: Let $\psi : \mathbb{N} \to \mathbb{R}^+$ be such that $\lim_n \psi(n) = 0$. Let $\alpha \in \mathbb{R}$ and suppose

$$\overset{\infty}{\exists}(p/q)\,|\alpha - (p/q)| < \psi(q).$$

If $\sum k\psi(k) < \infty$, then α cannot be random.

Properties of random continued fractions

- It turns out that random reals must be close to badly approximable.
- Theorem: Let $\psi : \mathbb{N} \to \mathbb{R}^+$ be such that $\lim_n \psi(n) = 0$. Let $\alpha \in \mathbb{R}$ and suppose

$$\overset{\infty}{\exists}(p/q)\, |\alpha - (p/q)| < \psi(q).$$

  If $\sum k\psi(k) < \infty$, then α cannot be random.
- This is an effective version of a theorem by Khintchine.