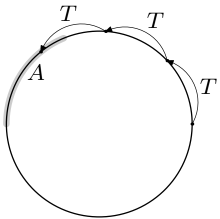
Ergodic-type characterization of randomness

Laurent Bienvenu (LIAFA, Paris),
Adam Day (Victoria University, Wellington)
Ilya Mezhirov (Technical Univ., Kaiserslautern)
Alexander Shen (LIF, Marseille)[1]

CiE 2010 (July 2010)

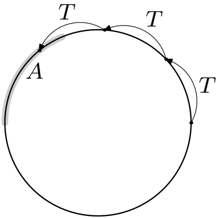
[1] on leave from IITP, Moscow

Ergodic theorem



X: space with measure μ
$T\colon X \to X$: measure preserving
$x, T(x), T(T(x)), T^3(x), \ldots$
how often in A?

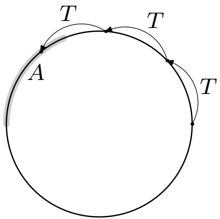
Ergodic theorem



X: space with measure μ
$T\colon X \to X$: measure preserving
$x, T(x), T(T(x)), T^3(x), \ldots$
how often in A?

Ergodic theorem: for almost every x there exists a limit frequency;

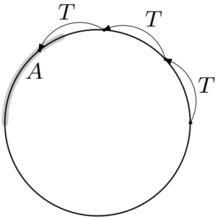
Ergodic theorem



X: space with measure μ
$T : X \to X$: measure preserving
$x, T(x), T(T(x)), T^3(x), \ldots$
how often in A?

Ergodic theorem: for almost every x there exists a limit frequency; it is $\mu(A)$ if T is ergodic (no invariant subspace)

Ergodic theorem

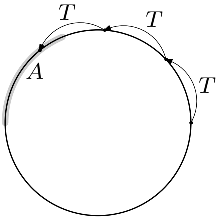


X: space with measure μ
$T: X \to X$: measure preserving
$x, T(x), T(T(x)), T^3(x), \ldots$
how often in A?

Ergodic theorem: for almost every x there exists a limit frequency; it is $\mu(A)$ if T is ergodic (no invariant subspace)

Example: how many powers of 2 start with digit 3?

Ergodic theorem



X: space with measure μ
$T : X \to X$: measure preserving
$x, T(x), T(T(x)), T^3(x), \ldots$
how often in A?

Ergodic theorem: for almost every x there exists a limit frequency; it is $\mu(A)$ if T is ergodic (no invariant subspace)
Example: how many powers of 2 start with digit 3?
answer: $log_{10}4 - \log_{10} 3$

Classical and algorithmic statements

Classical: "for almost every $x \ldots$"

Classical and algorithmic statements

Classical: "for almost every $x \dots$"
Effective: "for every algorithmicall random $x \dots$"

Classical and algorithmic statements

Classical: "for almost every x..."
Effective: "for every algorithmicall random x..."
Effective ergodic theorems: if T and A are good enough, for every (Martin-Löf) random x the limit frequency exists and is equal to $\mu(A)$

Classical and algorithmic statements

Classical: "for almost every x..."
Effective: "for every algorithmicall random x..."
Effective ergodic theorems: if T and A are good enough, for every (Martin-Löf) random x the limit frequency exists and is equal to $\mu(A)$
(Vyugin, Hoyrup, Rojas et al.)

Classical and algorithmic statements

Classical: "for almost every $x \ldots$"
Effective: "for every algorithmicall random $x \ldots$"
Effective ergodic theorems: if T and A are good enough, for every (Martin-Löf) random x the limit frequency exists and is equal to $\mu(A)$
(Vyugin, Hoyrup, Rojas et al.)
What we do: wider class of As, but weaker statement:
$\mu(A) < 1 \Rightarrow$ for every random x at least one of $x, T(x), T^2(x), \ldots$ is not in A

Kucera's theorem

Ω: Cantor space of infinite binary sequences

Kucera's theorem

Ω: Cantor space of infinite binary sequences
μ: uniform Bernoulli measure on Ω (independent fair coins)

Kucera's theorem

Ω: Cantor space of infinite binary sequences
μ: uniform Bernoulli measure on Ω (independent fair coins)
T: left shift, $T(x_0x_1x_2\ldots) = x_1x_2x_3\ldots$

Kucera's theorem

Ω: Cantor space of infinite binary sequences
μ: uniform Bernoulli measure on Ω (independent fair coins)
T: left shift, $T(x_0x_1x_2\ldots) = x_1x_2x_3\ldots$
T preserves μ

Kucera's theorem

Ω: Cantor space of infinite binary sequences
μ: uniform Bernoulli measure on Ω (independent fair coins)
T: left shift, $T(x_0x_1x_2\ldots) = x_1x_2x_3\ldots$
T preserves μ
$A \subset \Omega$: an effectively open set (union of a computable sequence of intervals); $\mu(A) < 1$.

Kucera's theorem

Ω: Cantor space of infinite binary sequences
μ: uniform Bernoulli measure on Ω (independent fair coins)
T: left shift, $T(x_0x_1x_2\dots) = x_1x_2x_3\dots$
T preserves μ
$A \subset \Omega$: an effectively open set (union of a computable sequence of intervals); $\mu(A) < 1$.
Kucera's theorem: if $x \in \Omega$ is Martin-Löf random, some tail $T^n(x)$ is outside A.

Kucera's theorem

Ω: Cantor space of infinite binary sequences
μ: uniform Bernoulli measure on Ω (independent fair coins)
T: left shift, $T(x_0x_1x_2\ldots) = x_1x_2x_3\ldots$
T preserves μ
$A \subset \Omega$: an effectively open set (union of a computable sequence of intervals); $\mu(A) < 1$.
Kucera's theorem: if $x \in \Omega$ is Martin-Löf random, some tail $T^n(x)$ is outside A.
$\Leftrightarrow$ If $T^n(x) \in A$ for every n, then x is not Martin-Löf random

Martin-Löf randomness

effectively null set N: for every $\varepsilon > 0$ one can effectively generate a sequence of intervals that cover N and have total measure $< \varepsilon$

Martin-Löf randomness

effectively null set N: for every $\varepsilon > 0$ one can effectively generate a sequence of intervals that cover N and have total measure $< \varepsilon$

Martin-Löf random: a sequence x that does not belong to effectively null set.

Martin-Löf randomness

effectively null set N: for every $\varepsilon > 0$ one can effectively generate a sequence of intervals that cover N and have total measure $< \varepsilon$

Martin-Löf random: a sequence x that does not belong to effectively null set.

Reformulation of Kucera's theorem: the set of all sequences x such that all tails of x are in A, is an effectively null set.

Variations on Kucera's theme

Let A be an effectively open set in Cantor space; $\mu(A) < 1$. Then for every ML-random x one may:

Variations on Kucera's theme

Let A be an effectively open set in Cantor space; $\mu(A) < 1$. Then for every ML-random x one may:

- (Kucera): delete some prefix of x to get $x' \notin A$

Variations on Kucera's theme

Let A be an effectively open set in Cantor space; $\mu(A) < 1$. Then for every ML-random x one may:

- (Kucera): delete some prefix of x to get $x' \notin A$
- change finitely many bits in x to get $x' \notin A$ (effective Kolmogorov 0-1-law)

Variations on Kucera's theme

Let A be an effectively open set in Cantor space; $\mu(A) < 1$. Then for every ML-random x one may:

- (Kucera): delete some prefix of x to get $x' \notin A$
- change finitely many bits in x to get $x' \notin A$ (effective Kolmogorov 0-1-law)
- add some finite prefix to x to get $x' \notin A$

Each of these properties can be used as characterization of randomness

General statement

Let $T\colon \Omega \to \Omega$ be a computable almost everywhere defined measure-preserving ergodic transformation of Cantor space (or the space of bi-infinite sequences) with a computable measure.

General statement

Let $T \colon \Omega \to \Omega$ be a computable almost everywhere defined measure-preserving ergodic transformation of Cantor space (or the space of bi-infinite sequences) with a computable measure.
Let A be an effectively open subset of Ω and $\mu(A) < 1$.

General statement

Let $T\colon \Omega \to \Omega$ be a computable almost everywhere defined measure-preserving ergodic transformation of Cantor space (or the space of bi-infinite sequences) with a computable measure.
Let A be an effectively open subset of Ω and $\mu(A) < 1$.
Then for every Martin-Löf random x there exists some $n \geq 0$ such that $T^n(x) \notin A$.

General statement

Let $T\colon \Omega \to \Omega$ be a computable almost everywhere defined measure-preserving ergodic transformation of Cantor space (or the space of bi-infinite sequences) with a computable measure.
Let A be an effectively open subset of Ω and $\mu(A) < 1$.
Then for every Martin-Löf random x there exists some $n \geq 0$ such that $T^n(x) \notin A$.

(In the proceedings T is required to be bijective; M. Hoyrup noted that it is not important.)

General statement and special cases

General statement and special cases

Changing bits: adding 1 in 2-adic notation (least significant bit is on the left)

General statement and special cases

Changing bits: adding 1 in 2-adic notation (least significant bit is on the left)

Adding prefix: shifts in the space of biinfinite sequence (van Lambalgen theorem is also needed)

General statement and special cases

Changing bits: adding 1 in 2-adic notation (least significant bit is on the left)

Adding prefix: shifts in the space of biinfinite sequence (van Lambalgen theorem is also needed)

Stronger claims in special cases: there are infinitely many shifts that move x outside A among any enumerable sequence of integers; statements about density of terms outside A

Application: Mijabe's result made easy

Theorem (Mijabe): let x^0 be a ML-random sequence, let x^1 be a ML-random sequence with oracle x^0, let x^2 be a ML-random sequence with oracle x^0, x^1 etc. Then one can change finitely many terms in each x^i in such a way that $x^0, x^1, \ldots$ is a random element of $\Omega \times \Omega \times \ldots$

Application: Mijabe's result made easy

Theorem (Mijabe): let x^0 be a ML-random sequence, let x^1 be a ML-random sequence with oracle x^0, let x^2 be a ML-random sequence with oracle x^0, x^1 etc. Then one can change finitely many terms in each x^i in such a way that $x^0, x^1, \ldots$ is a random element of $\Omega \times \Omega \times \ldots$

Now an easy consequence of the result about finite changes

Application: Mijabe's result made easy

Theorem (Mijabe): let x^0 be a ML-random sequence, let x^1 be a ML-random sequence with oracle x^0, let x^2 be a ML-random sequence with oracle x^0, x^1 etc. Then one can change finitely many terms in each x^i in such a way that $x^0, x^1, \ldots$ is a random element of $\Omega \times \Omega \times \ldots$

Now an easy consequence of the result about finite changes

Finite changes can be replaced by adding/deleting prefixes

Proof sketch

Let $A' = A \cap T^{-1}(A) \cap T^{-2}(A) \cap \ldots$.

Proof sketch

Let $A' = A \cap T^{-1}(A) \cap T^{-2}(A) \cap \dots$.
It is enough to find for every interval I a covering of $I \cap A'$ that has measure at most $(1 - \varepsilon)\mu(I)$

Proof sketch

Let $A' = A \cap T^{-1}(A) \cap T^{-2}(A) \cap \ldots$.
It is enough to find for every interval I a covering of $I \cap A'$ that has measure at most $(1-\varepsilon)\mu(I)$
We use effectively open set $I \cap (A \cap \ldots \cap T^{-N}(A))$ as this covering

Proof sketch

Let $A' = A \cap T^{-1}(A) \cap T^{-2}(A) \cap \ldots$.
It is enough to find for every interval I a covering of $I \cap A'$ that has measure at most $(1 - \varepsilon)\mu(I)$
We use effectively open set $I \cap (A \cap \ldots \cap T^{-N}(A))$ as this covering
Its measure is upperbounded by minimal $\mu(I \cap T^{-s}(A))$

Proof sketch

Let $A' = A \cap T^{-1}(A) \cap T^{-2}(A) \cap \ldots$.
It is enough to find for every interval I a covering of $I \cap A'$ that has measure at most $(1-\varepsilon)\mu(I)$
We use effectively open set $I \cap (A \cap \ldots \cap T^{-N}(A))$ as this covering
Its measure is upperbounded by minimal $\mu(I \cap T^{-s}(A))$
which is upperbounded by the average taken over all $s = 0, 1, \ldots, N$

Proof sketch

Let $A' = A \cap T^{-1}(A) \cap T^{-2}(A) \cap \ldots$.
It is enough to find for every interval I a covering of $I \cap A'$ that has measure at most $(1-\varepsilon)\mu(I)$
We use effectively open set $I \cap (A \cap \ldots \cap T^{-N}(A))$ as this covering
Its measure is upperbounded by minimal $\mu(I \cap T^{-s}(A))$
which is upperbounded by the average taken over all $s = 0, 1, \ldots, N$
which is estimated using erdodic theorem for I and computability