Oscillation-free CHAITIN h-random sequences

Ludwig Staiger

Martin-Luther-Universität Halle-Wittenberg

International Workshop on Theoretical Computer Science

February 23, 2012, Auckland, New Zealand

Outline

Foreword

Foreword

Dedicated to Professor S. Marcus on the occasion of his 60th birthday

P. MARTIN-LÖF TESTS: REPRESENTABILITY AND EMBEDDABILITY

CRISTIAN CALUDE, ION CHIŢESCU and LUDWIG STAIGER

There are several ways to compute the complexity of a program [6]. One of them is due to Kolmogorov (see [7] and [5], [8], [12]). Another one is due to P. Martin-Löf (see [9] and [14], [15], [1]). These patterns of computing complexity are in fact closely related. For a comparison of these approaches for infinite sequences, see [11]. The main purpose of this paper is to present in a systematic way some results concerning the connection between Kolmogorov's and P. Martin-Löf's theories for strings. We work within the general framework of a not necessarily binary alphabet [1].

The first two authors acknowledge valuable discussions with professor S. Marcus.

REV. ROUMAINE MATH. PURES APPL. 30(1985), 719–732

Notation: Strings and Languages

Finite Alphabet $X = \{0, \dots, r-1\}$, cardinality $|X| = r$

Finite strings (words) $w = x_1 \cdots x_n \in X^*$, $x_i \in X$

Length $|w| = n$

Languages $W \subseteq X^*$

Notation: Strings and Languages

Finite Alphabet $X = \{0, \ldots, r-1\}$, cardinality $|X| = r$

Finite strings (words) $w = x_1 \cdots x_n \in X^*$, $x_i \in X$

Length $|w| = n$

Languages $W \subseteq X^*$

Infinite strings (ω-words) $\mathbf{x} = x_1 \cdots x_n \cdots \in X^\omega$

Prefixes of infinite strings $\mathbf{x}[0..n] \in X^*$, $\left|\mathbf{x}[0..n]\right| = n$

ω-Languages $F \subseteq X^\omega$

X^ω as CANTOR space

Metric: $\rho(\mathbf{y},\mathbf{x}) := \inf\{r^{-|w|} : w \in \mathrm{pref}(\mathbf{y}) \cap \mathrm{pref}(\mathbf{x})\}$

Balls: $w \cdot X^\omega = \{\mathbf{y} : w \in \mathrm{pref}(\mathbf{y})\}$

Diameter: $\mathrm{diam}\, w \cdot X^\omega = r^{-|w|}$

$\mathrm{diam}\, F = \inf\{r^{-|w|} : F \subseteq w \cdot X^\omega\}$

Open sets: $W \cdot X^\omega = \bigcup_{w \in W} w \cdot X^\omega$

Closure: $\mathcal{C}(F) = \{\mathbf{x} : \mathrm{pref}(\mathbf{x}) \subseteq \mathrm{pref}(F)\}$

Description complexity: plain *or* simple complexity

Definition (Description complexity K_φ)

Let $\varphi :\subseteq X^* \to X^*$ *be a partial computable function.*

$$K_\varphi(w) := \inf\{|\pi| : \varphi(\pi) = w\}$$

Definition (Plain or Simple universal machine)

A machine (mapping) $\mathfrak{U}_S :\subseteq X^* \to X^*$ *is called* **universal** *if and only if for every partial computable mapping* $\varphi :\subseteq X^* \to X^*$ *there is a constant* c_φ *such that*

$$\forall w (K_\varphi(w) \le K_{\mathfrak{U}_S}(w) + c_\varphi)\,.$$

Description complexity: plain *or* simple complexity

Definition (Description complexity K_φ)

Let $\varphi :\subseteq X^* \to X^*$ be a partial computable function.

$$K_\varphi(w) := \inf\{|\pi| : \varphi(\pi) = w\}$$

Definition (Plain or Simple universal machine)

A machine (mapping) $\mathfrak{U}_S :\subseteq X^* \to X^*$ is called **universal** *if and only if for every partial computable mapping $\varphi :\subseteq X^* \to X^*$ there is a constant c_φ such that*

$$\forall w(K_\varphi(w) \le K_{\mathfrak{U}_S}(w) + c_\varphi).$$

Definition (Plain or Simple description complexity)

$$\mathrm{KS}(w) := \min\{|\pi| : \mathfrak{U}_S(\pi) = w\}$$

Description complexity: prefix complexity

Definition (Prefix-free universal machine)

A prefix-free machine (mapping) $\mathfrak{U}_P :\subseteq X^* \to X^*$ *is called* **universal** *if and only if*

1. $\mathrm{dom}(\mathfrak{U}_P)$ *is prefix-free, and*
2. *for every partial computable mapping* $\varphi :\subseteq X^* \to X^*$ *with prefix-free domain* $\mathrm{dom}(\varphi)$ *there is a constant* c_φ *such that*

$$\forall w (K_\varphi(w) \leq K_{\mathfrak{U}_P}(w) + c_\varphi) .$$

Description complexity: prefix complexity

Definition (Prefix-free universal machine)

A prefix-free machine (mapping) $\mathfrak{U}_P :\subseteq X^* \to X^*$ is called **universal** *if and only if*

1. $\mathrm{dom}(\mathfrak{U}_P)$ *is prefix-free, and*
2. *for every partial computable mapping $\varphi :\subseteq X^* \to X^*$ with prefix-free domain $\mathrm{dom}(\varphi)$ there is a constant c_φ such that*

$$\forall w (K_\varphi(w) \leq K_{\mathfrak{U}_P}(w) + c_\varphi) .$$

Definition (Prefix-free description complexity)

$$\mathrm{KP}(w) := \min\{|\pi| : \mathfrak{U}_P(\pi) = w\}$$

a priori-complexity

Definition (Semi-measure)

$\nu : X^* \to \mathbb{R}$ is a (*cylindrical*) *semi-measure* provided

$$\forall w(w \in X^* \wedge x \in X \to \nu(w) \geq \sum_{x \in X} \nu(wx)).$$

Theorem (Levin'70)

There is a universal left computable semi-measure **M**, *that is, for every left computable semi-measure* ν *there is a constant* c_ν *such that*

$$\forall w(w \in X^* \to \nu(w) \leq c_\nu \cdot \mathbf{M}(w)).$$

a priori-complexity

Definition (Semi-measure)

$\nu : X^* \to \mathbb{R}$ is a (*cylindrical*) ***semi-measure*** provided

$$\forall w (w \in X^* \land x \in X \to \nu(w) \geq \sum_{x \in X} \nu(wx)).$$

Theorem (Levin'70)

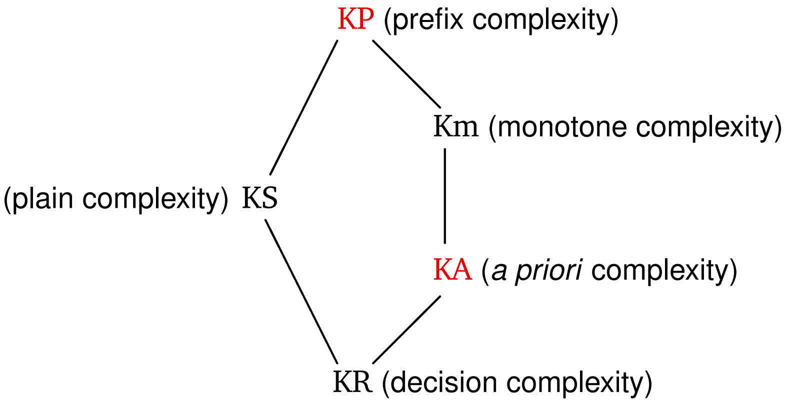
There is a universal left computable semi-measure **M**, *that is, for every left computable semi-measure ν there is a constant c_ν such that*

$$\forall w (w \in X^* \to \nu(w) \leq c_\nu \cdot \mathbf{M}(w)).$$

Definition (*a priori*-complexity)

$$\mathrm{KA}(w) := -\log_{|X|} \mathbf{M}(w)$$

Uspensky–Shen–Pentagon



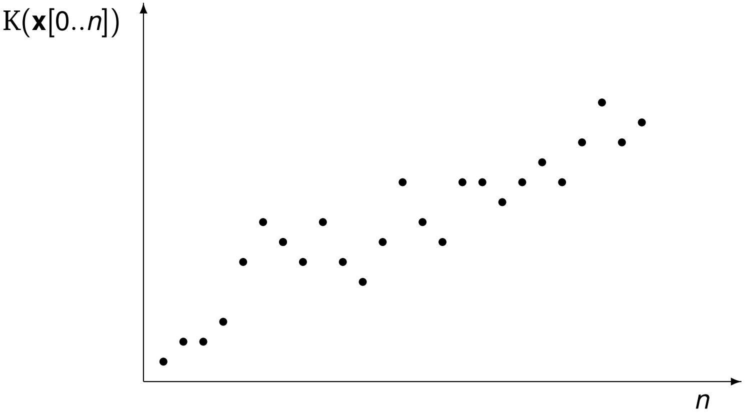
Simple Relations Between Complexities

Properties

1. $|\mathrm{KS}(w) - \mathrm{KS}(wx)| \leq O(1)$ and
   $|\mathrm{KP}(w) - \mathrm{KP}(wx)| \leq O(1)$
2. $\mathrm{KA}(w) \leq \mathrm{KA}(wx)$
3. $0 \leq \mathrm{KS}(w), \mathrm{KA}(w) \leq |w| + O(1)$
4. $\mathrm{KS}(w), \mathrm{KA}(w) \leq \mathrm{KP}(w) + O(1)$
5. $\mathrm{KP}(w) \leq \mathrm{KS}(w) + O(\log_{|X|} |w|)$
6. $\mathrm{KP}(w) \leq \mathrm{KA}(w) + O(\log_{|X|} |w|)$

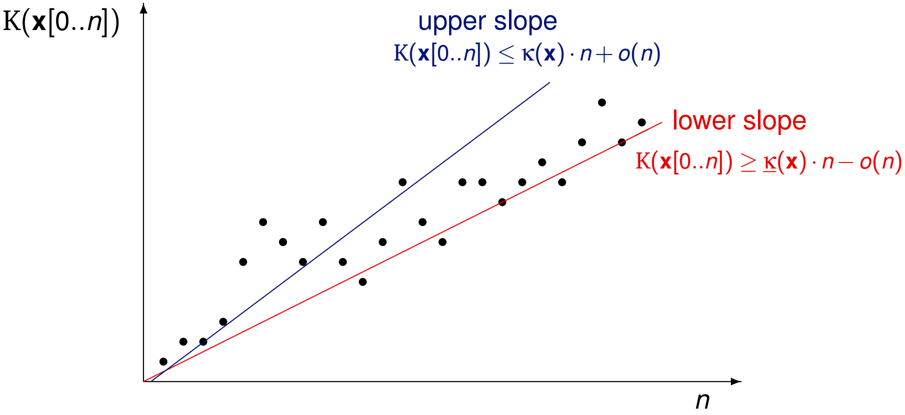
Complexity of infinite words

Plot of the function $K(\mathbf{x}[0..n])$



Complexity of infinite words

Plot of the function $\mathrm{K}(\mathbf{x}[0..n])$



Asymptotic complexity

$$\underline{\kappa}(\mathbf{x}) := \liminf_{n\to\infty} \frac{\mathrm{K}(\mathbf{x}[0..n])}{n} \qquad \kappa(\mathbf{x}) := \limsup_{n\to\infty} \frac{\mathrm{K}(\mathbf{x}[0..n])}{n}$$

Random sequences

Theorem

Let $\mathbf{x} \in X^\omega$. Then $\mathbf{x}$ is random if and only if one of the following conditions is satisfied.

Random sequences

Theorem

Let $\mathbf{x} \in X^{\omega}$. Then $\mathbf{x}$ is random if and only if one of the following conditions is satisfied.

for prefix complexity $\mathrm{KP}(\mathbf{x}[0..n]) \geq n - O(1)$

Random sequences

Theorem

Let $\mathbf{x} \in X^{\omega}$. *Then* $\mathbf{x}$ *is random if and only if one of the following conditions is satisfied.*

for prefix complexity $\mathrm{KP}(\mathbf{x}[0..n]) \geq n - O(1)$

or more precise $\lim_{n\to\infty} \mathrm{KP}(\mathbf{x}[0..n]) - n = \infty$.

Random sequences

Theorem

Let $\mathbf{x} \in X^{\omega}$*. Then* $\mathbf{x}$ *is random if and only if one of the following conditions is satisfied.*

for prefix complexity $\mathrm{KP}(\mathbf{x}[0..n]) \geq n - O(1)$

or more precise $\lim_{n\to\infty} \mathrm{KP}(\mathbf{x}[0..n]) - n = \infty.$

for *a priori* complexity $\mathrm{KA}(\mathbf{x}[0..n]) \geq n - O(1)$

Random sequences

Theorem

Let $\mathbf{x} \in X^\omega$. Then $\mathbf{x}$ is random if and only if one of the following conditions is satisfied.

for prefix complexity $\mathrm{KP}(\mathbf{x}[0..n]) \geq n - O(1)$

or more precise $\lim_{n\to\infty} \mathrm{KP}(\mathbf{x}[0..n]) - n = \infty$.

for *a priori* complexity $\mathrm{KA}(\mathbf{x}[0..n]) \geq n - O(1)$

or more precise $\left|\mathrm{KA}(\mathbf{x}[0..n]) - n\right| \leq O(1)$

Partial randomness

Definition (Tadaki 2002, Calude et al. 2006)

Let $\mathbf{x} \in X^{\omega}$ and $1 \geq \varepsilon > 0$. Then $\mathbf{x}$ is

weakly CHAITIN ε-random or **weakly MARTIN-LÖF ε-random** if

$$\mathrm{KP}(\mathbf{x}[0..n]) \geq \varepsilon \cdot n - O(1),$$

Partial randomness

Definition (Tadaki 2002, Calude et al. 2006)

Let $\mathbf{x} \in X^\omega$ and $1 \geq \varepsilon > 0$. Then $\mathbf{x}$ is

weakly Chaitin ε-random or **weakly Martin-Löf ε-random** if

$$\mathrm{KP}(\mathbf{x}[0..n]) \geq \varepsilon \cdot n - O(1),$$

strongly Chaitin ε-random if $\lim_{n\to\infty} \mathrm{KP}(\mathbf{x}[0..n]) - \varepsilon \cdot n = \infty$,

Partial randomness

Definition (Tadaki 2002, Calude et al. 2006)

Let $\mathbf{x} \in X^\omega$ and $1 \geq \varepsilon > 0$. Then $\mathbf{x}$ is

weakly Chaitin ε-random or **weakly Martin-Löf ε-random** if

$$\mathrm{KP}(\mathbf{x}[0..n]) \geq \varepsilon \cdot n - O(1),$$

strongly Chaitin ε-random if $\lim_{n\to\infty} \mathrm{KP}(\mathbf{x}[0..n]) - \varepsilon \cdot n = \infty$,

strongly Martin-Löf ε-random if $\mathrm{KA}(\mathbf{x}[0..n]) \geq \varepsilon \cdot n - O(1)$.

Partial randomness

Definition (Tadaki 2002, Calude et al. 2006)

Let $\mathbf{x} \in X^\omega$ and $1 \geq \varepsilon > 0$. Then $\mathbf{x}$ is

weakly CHAITIN ε-random or **weakly MARTIN-LÖF ε-random** if

$$\mathrm{KP}(\mathbf{x}[0..n]) \geq \varepsilon \cdot n - O(1),$$

strongly CHAITIN ε-random if $\lim_{n\to\infty} \mathrm{KP}(\mathbf{x}[0..n]) - \varepsilon \cdot n = \infty$,

strongly MARTIN-LÖF ε-random if $\mathrm{KA}(\mathbf{x}[0..n]) \geq \varepsilon \cdot n - O(1)$.

Theorem (Reimann & Stephan)

Strongly MARTIN-LÖF *ε-random* $\Rightarrow$ *strongly* CHAITIN *ε-random* $\Rightarrow$ *weakly* CHAITIN *ε-random, and none of the implications can be reversed if* $0 < \varepsilon < 1$ *is computable.*

Oscillation-free ε-random sequences

Definition (Oscillation-freeness)

An ω-word $\mathbf{x} \in X^{\omega}$ is called *oscillation-free* CHAITIN ε-*random* provided

$$|\mathrm{KP}(\mathbf{x}[0..n]) - \varepsilon \cdot n| \leq O(1) \text{ , and}$$

it is called *oscillation-free* MARTIN-LÖF ε-*random* provided

$$|\mathrm{KA}(\mathbf{x}[0..n]) - \varepsilon \cdot n| \leq O(1)\,.$$

Oscillation-free ε-random sequences

Definition (Oscillation-freeness)

An ω-word $\mathbf{x} \in X^\omega$ is called *oscillation-free* CHAITIN ε-*random* provided

$$|\mathrm{KP}(\mathbf{x}[0..n]) - \varepsilon \cdot n| \le O(1) \text{ , and}$$

it is called *oscillation-free* MARTIN-LÖF ε-*random* provided

$$|\mathrm{KA}(\mathbf{x}[0..n]) - \varepsilon \cdot n| \le O(1) \,.$$

Theorem (*St'08, Tadaki 2010, Calude et al. 2011*)

If $0 < \varepsilon < 1$ *is computable then there are oscillation-free* MARTIN-LÖF *ε-random and oscillation-free* CHAITIN *ε-random ω-words.*

Dilution

Modulus function: $g : \mathbb{N} \to \mathbb{N}$ strictly monotone, that is, $g(n+1) > g(n)$

Definition (Dilution function $\varphi : X^* \to X^*$)

$$\begin{aligned} \varphi(e) &:= 0^{g(0)} \text{ and} \\ \varphi(wx) &:= \varphi(w) \cdot x \cdot 0^{g(n+1)-g(n)-1} \end{aligned}$$

Dilution

Modulus function: $g : \mathbb{N} \to \mathbb{N}$ strictly monotone, that is, $g(n+1) > g(n)$

Definition (Dilution function $\varphi : X^* \to X^*$)

$$\begin{aligned} \varphi(e) &:= 0^{g(0)} \text{ and} \\ \varphi(wx) &:= \varphi(w) \cdot x \cdot 0^{g(n+1)-g(n)-1} \end{aligned}$$

Theorem (*St*'09)

Let $\varphi : X^* \to X^*$ be a computable dilution function with modulus function $g : \mathbb{N} \to \mathbb{N}$ and let $\mathrm{K} \in \{\mathrm{KP}, \mathrm{KS}, \mathrm{KA}\}$. Then

$$\left|\mathrm{K}\big(\overline{\varphi}(\mathbf{x})[0..g(n)]\big) - \mathrm{K}\big(\mathbf{x}[0..n]\big)\right| \leq O(1)$$

for all $\mathbf{x} \in X^\omega$ and all $n \in \mathbb{N}$.

Hausdorff dimension and partial randomness

Relations between "usual" Hausdorff dimension and the lower asymptotic complexity $\underline{\kappa}$

- RYBAKO 1984, 1986
- CAI & HARTMANIS 1994
- *St.* 1993, 1998
- LUTZ 2000, 2003
- HITCHCOCK 2005

Hausdorff dimension and partial randomness

Relations between "usual" Hausdorff dimension and the lower asymptotic complexity $\underline{\kappa}$

- RYBAKO 1984, 1986
- CAI & HARTMANIS 1994
- *St.* 1993, 1998
- LUTZ 2000, 2003
- HITCHCOCK 2005

Relations between "usual" Hausdorff dimension and complexity functions for automaton-definable ω-languages $F \subseteq X^\omega$ [*St*93, 08]

The complexity functions $\mathrm{K}(\mathbf{x}[0..n]), \mathbf{x} \in F$, reflect the scaled down by $\varepsilon = \dim_H F$ behaviour of $\mathrm{K}(\mathbf{y}[0..n]), \mathbf{y} \in X^\omega$.

Refining the scale – original Hausdorff dimension

Definition (Gauge functions [HAUSDORFF 1918])

A function $h : (0, \infty) \to (0, \infty)$ is a *gauge function* if h is right continuous and non-decreasing.

Refining the scale – original Hausdorff dimension

Definition (Gauge functions [HAUSDORFF 1918])

A function $h : (0,\infty) \to (0,\infty)$ is a *gauge function* if h is right continuous and non-decreasing.

Example

$$\begin{aligned} h_\varepsilon(t) &:= t^\varepsilon \qquad \text{is a gauge function.} \\ -\log_r h_\varepsilon(r^{-n}) &= \varepsilon \cdot n \end{aligned}$$

Refining the scale – original Hausdorff dimension

Definition (Gauge functions [HAUSDORFF 1918])

A function $h : (0, \infty) \to (0, \infty)$ is a *gauge function* if h is right continuous and non-decreasing.

Example

$$\begin{aligned} h_\varepsilon(t) &:= t^\varepsilon \qquad \text{is a gauge function.} \\ -\log_r h_\varepsilon(r^{-n}) &= \varepsilon \cdot n \end{aligned}$$

Functions of the logarithmic scale [HAUSDORFF 1918]

$$h_{(p_0,\ldots,p_k)}(t) = t^{p_0} \cdot \prod_{i=1}^{k} (\log^i \frac{1}{t})^{p_i}$$

First nonzero p_i is positive.

Gauge functions and modulus functions

Lemma (*St'11*)

Let $r \in \mathbb{N}, r \geq 2$, *and* $h : (0, \infty) \cap \mathbb{Q} \to \mathbb{R}$ *be a (computable) gauge function satisfying the conditions*

1. $1 < h(1) < r$ *and*
2. *for every* $j \in \mathbb{N}$ *there is an* $m \in \mathbb{N}$ *such that* $r^{-j} < h(r^{-m}) \leq r^{-j+1}$.

Then there is a (computable) modulus function $g : \mathbb{N} \to \mathbb{N}$ *such that* $r^{-n-1} < h(r^{-g(n)}) < r^{-n+1}$, *for all* $n \in \mathbb{N}$.

Gauge functions and modulus functions

Lemma (*St'11*)

Let $r \in \mathbb{N}, r \geq 2$, *and* $h : (0, \infty) \cap \mathbb{Q} \to \mathbb{R}$ *be a (computable) gauge function satisfying the conditions*

1. $1 < h(1) < r$ *and*
2. *for every* $j \in \mathbb{N}$ *there is an* $m \in \mathbb{N}$ *such that* $r^{-j} < h(r^{-m}) \leq r^{-j+1}$.

Then there is a (computable) modulus function $g : \mathbb{N} \to \mathbb{N}$ *such that* $r^{-n-1} < h(r^{-g(n)}) < r^{-n+1}$, *for all* $n \in \mathbb{N}$.

Sufficient condition

$h : (0, \infty) \cap \mathbb{Q} \to \mathbb{R}$ is $\cap$-convex and $h(t) > t$

Oscillation-free *h*-random ω-words

Definition (Oscillation-freeness)

Let $h : (0,\infty) \cap \mathbb{R} \to \mathbb{R}$ be a gauge function and $r = |X|$. An ω-word $\mathbf{x} \in X^\omega$ is called *oscillation-free* CHAITIN *h-random* provided

$$|\mathrm{KP}(\mathbf{x}[0..n]) - (-\log_r h(r^{-n}))| \leq O(1) \text{ , and}$$

$\mathbf{x} \in X^\omega$ is called *oscillation-free* MARTIN-LÖF *h-random* provided

$$|\mathrm{KA}(\mathbf{x}[0..n]) - (-\log_r h(r^{-n}))| \leq O(1) \,.$$

Oscillation-free h-random ω-words

Definition (Oscillation-freeness)

Let $h : (0,\infty) \cap \mathbb{R} \to \mathbb{R}$ be a gauge function and $r = |X|$. An ω-word $\mathbf{x} \in X^\omega$ is called *oscillation-free* CHAITIN *h-random* provided

$$|\mathrm{KP}(\mathbf{x}[0..n]) - (-\log_r h(r^{-n}))| \leq O(1) \text{ , and}$$

$\mathbf{x} \in X^\omega$ is called *oscillation-free* MARTIN-LÖF *h-random* provided

$$|\mathrm{KA}(\mathbf{x}[0..n]) - (-\log_r h(r^{-n}))| \leq O(1) .$$

Theorem (*St'11*)

If $g : \mathbb{N} \to \mathbb{N}$ is a computable modulus function and $h : (0,\infty) \cap \mathbb{Q} \to \mathbb{R}$ is a corresponding computable gauge function then there are oscillation-free MARTIN-LÖF *h-random ω-words.*

KP-moderate gauge functions

Definition (KP-moderate gauge functions)

We refer a gauge function $h : \mathbb{Q} \cap (0, \infty) \to \mathbb{N}$ as KP-*moderate* if for every $d \in \mathbb{N}$ there is an ℓ_d such that the inequality

$$\mathrm{KP}(n) + d - 1 \leq -\log_r \frac{h(r^{-(n+\ell)})}{h(r^{-\ell})} \leq n - \big(\mathrm{KP}(n) + d - 1\big) \qquad (1)$$

holds for all $\ell \geq \ell_d$ and, depending on the value of d, for all sufficiently large $n \in \mathbb{N}$.

KP-moderate gauge functions

Definition (KP-moderate gauge functions)

We refer a gauge function $h : \mathbb{Q} \cap (0,\infty) \to \mathbb{N}$ as KP-*moderate* if for every $d \in \mathbb{N}$ there is an ℓ_d such that the inequality

$$\mathrm{KP}(n) + d - 1 \leq -\log_r \frac{h(r^{-(n+\ell)})}{h(r^{-\ell})} \leq n - \big(\mathrm{KP}(n) + d - 1\big) \qquad (1)$$

holds for all $\ell \geq \ell_d$ and, depending on the value of d, for all sufficiently large $n \in \mathbb{N}$.

Property [Sufficient condition]

If there are $\gamma, \bar{\gamma}$, $0 < \gamma \leq \bar{\gamma} < 1$, such that

$$\gamma^n \cdot h(r^{-\ell}) \leq h(r^{-n} \cdot r^{-\ell}) \leq \bar{\gamma}^n \cdot h(r^{-\ell}) \text{ for all } n \in \mathbb{N}$$

then h is KP-moderate.

Results: existence theorems

Theorem

Let $h : \mathbb{Q} \cap (0,\infty) \to \mathbb{R}$ *be a* KP*-moderate gauge function and* $r = |X|$*. Then there is an* ω*-word* $\mathbf{x} \in X^\omega$ *and a constant* c_h *such that*

$$|\mathrm{KP}(\mathbf{x}[0..n]) - (-\log_r h(r^{-n}))| \leq c_h .$$

Results: existence theorems

Theorem

Let $h : \mathbb{Q} \cap (0, \infty) \to \mathbb{R}$ *be a* KP*-moderate gauge function and* $r = |X|$*.*
Then there is an ω*-word* $\mathbf{x} \in X^\omega$ *and a constant* c_h *such that*

$$|\mathrm{KP}(\mathbf{x}[0..n]) - (-\log_r h(r^{-n}))| \leq c_h \,.$$

Theorem

Let $h : \mathbb{Q} \cap (0, \infty) \to \mathbb{R}$ *be a computable* KP*-moderate gauge function.*
Then there exists an oscillation-free Chaitin h-random ω*-word* $\mathbf{x} \in X^\omega$ *such that* $0\,.\mathbf{x}$ *is a left computable real.*

Results: a separation theorem

Theorem

Let $h : \mathbb{Q} \cap (0, \infty) \to \mathbb{R}$ *be a computable* KP*-moderate gauge function.*
Then there exists a Π^0_1*-definable* ω*-language which contains an oscillation-free Martin-Löf h-random* ω*-word* ξ *but no oscillation-free Chaitin h-random* ω*-word.*