Randomness and Compressibility

Akhil S

When can you say that a sequences is random?

(1) 0101010101010101 . . .

(2) 00101101110111101111 . . .

(3) 0100011011000001010011 . . .

(4) 00100100011111101101 . . .

Overview

- Randomness = (in)compressibility

Overview

- Randomness = (in)compressibility
- Rate of randomness = rate of (in)compressibility

Overview

- Randomness = (in)compressibility
- Rate of randomness = rate of (in)compressibility
- Polynomial-time rates of

  $$\text{Randomness} \stackrel{?}{=} \text{(in)compressibility}$$

Overview

- Randomness = (in)compressibility
- Rate of randomness = rate of (in)compressibility
- Polynomial-time rates of

  $$\text{Randomness} \stackrel{?}{=} \text{(in)compressibility}$$

- One-way functions

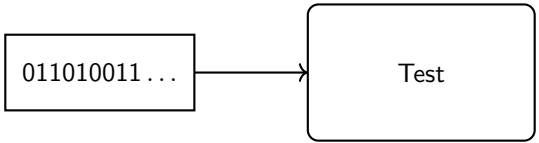
Randomness

Philosophy

Something is random

if it looks random to you.

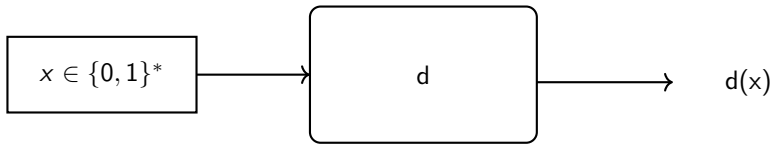
Test of randomness



X is Random $\iff$ $T(X)$ *fails.*

All "random" strings must fail T

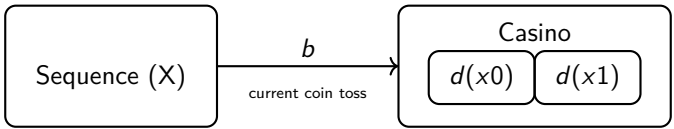
Test of randomness: Martingales



Fair betting : $d(x.0) + d(x.1) = 2 \cdot d(x)$.

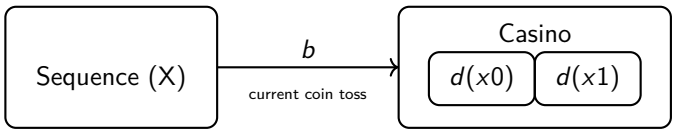
d is "effective".

Martingales as a casino game



$$2.d(x) = d(x0) + d(x1)$$

Martingales as a casino game



X is Martin-Löf Random $\iff$ *for all effective* d, $\limsup d(X \upharpoonright n) < \infty$.

Philosophy

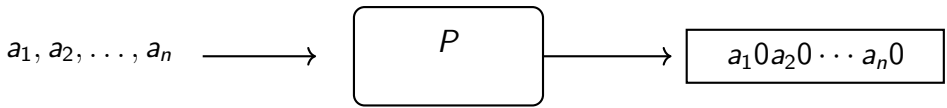
Something is random

if it is incompressible to you.

Kolmogorov complexity

$x := a_1.0.a_2.0 \ldots a_n.0$

Kolmogorov complexity

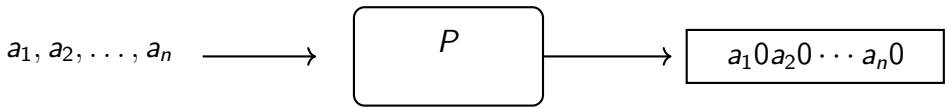


Kolmogorov complexity

$$K(x) \;=\; \min\{\, |p| \;:\; U(p) = x \,\}$$

length of the shortest program producing x

Kolmogorov complexity



$$K(a_1.0.a_2.0, \ldots, a_n.0) \leq n + O(1)$$

Randomness = incompressibility

Theorem : X is MLR $\iff \forall n\, K(X\restriction n) \geq n - O(1)$

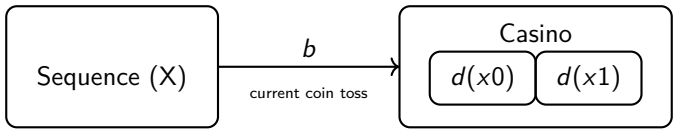
Example

$$X := a_1.0.a_2.0 \dots a_n.0 \dots$$

$$\forall n, \quad K(X \upharpoonright n) \leq n/2 + O(1)$$

Example

$X := a_1.0.a_2.0 \ldots a_n.0 \ldots$



$$2.d(x) = d(x0) + d(x1)$$

Example

$X := a_1.0.a_2.0 \ldots a_n.0 \ldots$ $\qquad d(\lambda) = 1$

$$\text{If } |x| \text{ is even:} \quad \begin{aligned} d(x0) &= 2\, d(x) \\ d(x1) &= 0\, d(x) \end{aligned}$$

Example

$X := a_1.0.a_2.0 \ldots a_n.0 \ldots$ $\qquad d(\lambda) = 1$

$$\text{If } |x| \text{ is even:} \quad d(x0) = 2\, d(x)$$
$$d(x1) = 0\, d(x)$$

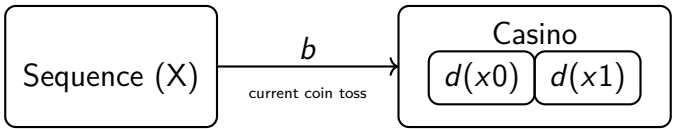
$$\text{If } |x| \text{ is odd:} \quad d(xb) = d(x)$$

Bet the entire amount only on the even 0*'s*

Rate of Randomness

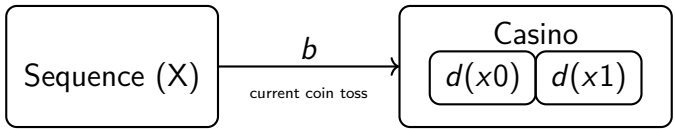
Stingy Casino : s-gale

$$X := a_1.0.a_2.0 \ldots a_n.0 \ldots$$



Stingy Casino : s-gale

$$X := a_1.0.a_2.0 \ldots a_n.0 \ldots$$



$$2^s\, d(x) = d(x0) + d(x1) \qquad s \in (0, 1]$$

Example

$X := a_1.0.a_2.0 \ldots a_n.0 \ldots$ $\qquad s = 0.5$

$$\text{If } |x| \text{ is even:} \quad \begin{aligned} d(x0) &= \sqrt{2}\, d(x) \\ d(x1) &= 0\, d(x) \end{aligned}$$

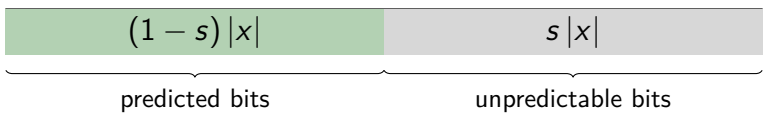
$$\text{If } |x| \text{ is odd:} \quad d(xb) = \frac{1}{\sqrt{2}} d(x)$$

Bet the entire amount only on the even 0*'s*

s-gales : Fast winning Martingales

$$d(x) \text{ is a martingale} \iff \tilde{d}(x) = 2^{(s-1)|x|}\, d(x) \text{ is an } s\text{-gale}$$

$$\tilde{d}(x) > 1 \iff d(x) > 2^{(1-s)|x|}$$



Constructive dimension

$$\dim(X) \;=\; \inf\{\, s \;:\; \exists \text{ effective } s\text{-gale } d \text{ that succeeds on } X \,\}$$

d succeeds on X iff $\limsup_n d(X \upharpoonright n) = \infty$

Constructive dimension

$$\dim(X) \;=\; \liminf_{n\to\infty} \frac{K(X \upharpoonright n)}{n}$$

rate of algorithmic randomness

Example

$X := a_1.0.a_2.0 \ldots a_n.0 \ldots$

$K(X \upharpoonright n) \leq n/2 + O(1)$

$$\dim(X) \leq 1/2$$

Hausdorff dimension

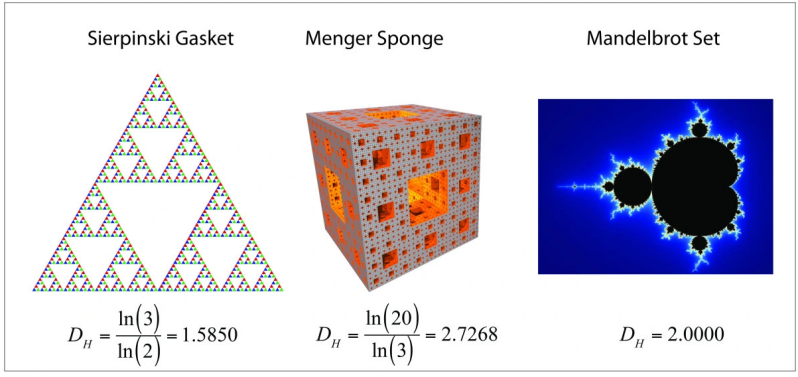


Image source: `https://galileo-unbound.blog/wp-content/uploads/2020/12/fractals.jpg`

Point-to-Set Principle

$$\dim_H(E) = \min_A \sup_{x \in E} \dim^A(x)$$

fractal dimension via algorithmic randomness of points

Applications : Information theoretic proofs of Kakeya Conjecture, Mastrand's Projection theorems, Distance sets, Faithfulness.

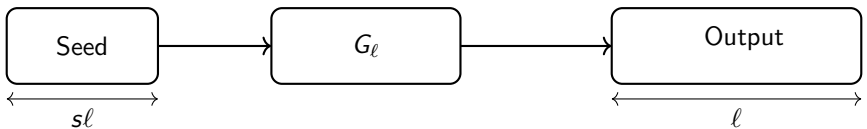
Summary

- Randomness = (in)compressibility
  - Martingale fail $\iff$ Maximal K.C
- Rates of randomness = rate of (in)compressibility
  - $s - gale$ fail $\iff$ Rate of K.C $> s$

Pseudo-Randomness

Pseudorandom generators

$$\text{PRG}: \quad \{G_\ell : \{0,1\}^{s\cdot\ell} \to \{0,1\}^{\ell}\}_{\ell\in\mathbb{N}} \qquad s \in (0,1)$$



Constant-stretch pseudorandom generator

$$G : \{0,1\}^{sn} \longrightarrow \{0,1\}^{n} \quad (0 < s < 1)$$

Definition. G is a cryptographic PRG if for all PPT D:

Constant-stretch pseudorandom generator

$$G : \{0,1\}^{sn} \longrightarrow \{0,1\}^{n} \quad (0 < s < 1)$$

Definition. G is a cryptographic PRG if for all PPT D:

$$\Big|\Pr[D(\text{ PRG String}) = 1] - \Pr[D(\text{True random string}) = 1]\Big| \leq \text{negl}(n)$$

polynomial-time indistinguishable from uniform

Constant-stretch pseudorandom generator

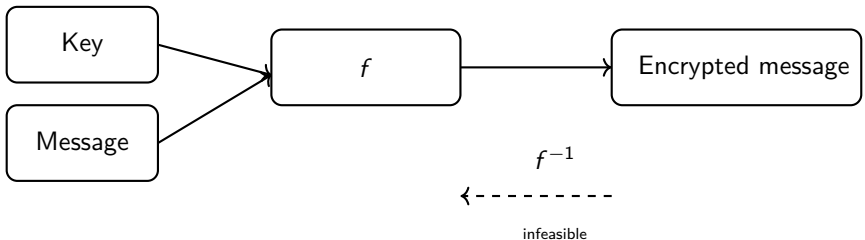
$$G : \{0,1\}^{sn} \longrightarrow \{0,1\}^{n} \quad (0 < s < 1)$$

Definition. G is a cryptographic PRG if for all PPT D:

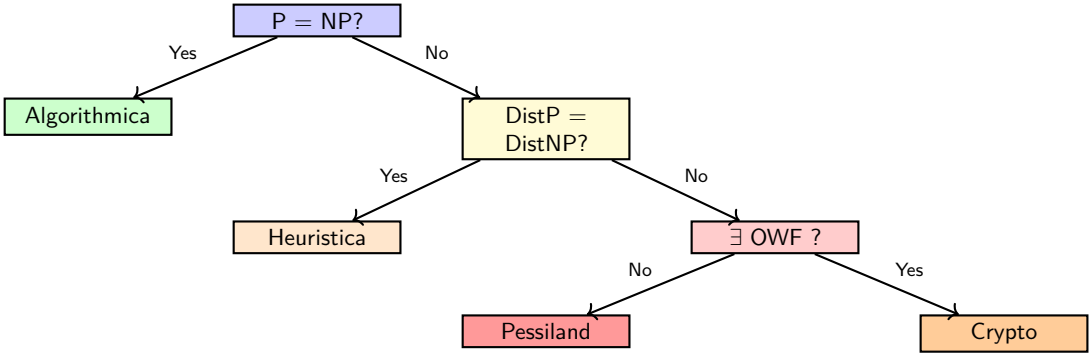
$$\left| \Pr[D(G(U_{sn})) = 1] - \Pr[D(U_n) = 1] \right| \leq \mathrm{negl}(n)$$

One-way functions

f is one-way if $f(x) = y$ is easy to compute, but $f^{-1}(y) = x$ is hard to compute



Impagliazzo's Five Worlds



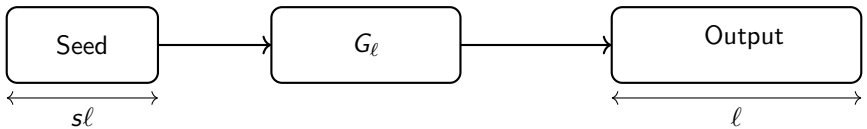
Pseudorandomness and Information

Time-bounded Kolmogorov complexity

$$K^t(x) \;=\; \min\{\, |p| \;:\; U(p) = x \text{ in time } t(|x|)\,\}$$

Pseudorandom generators

$$\text{PRG}: \quad \{G_\ell : \{0,1\}^{s\cdot\ell} \to \{0,1\}^\ell\}_{\ell\in\mathbb{N}} \qquad s \in (0,1)$$

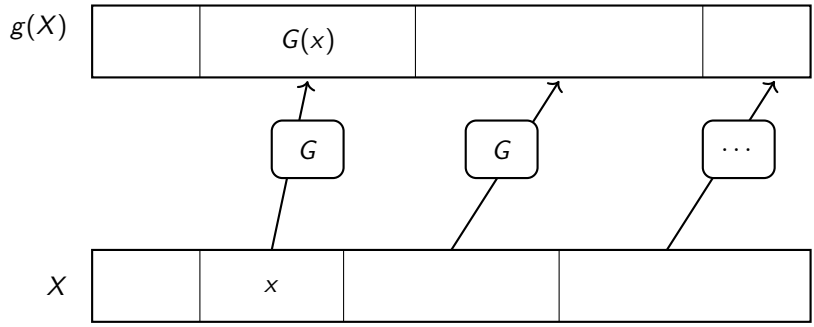


$$K_t(Output) \leq s\ell + O(1)$$

Time-bounded Kolmogorov complexity rate

$$\mathcal{K}_{poly}(X) = \inf_{t \in poly} \liminf_{n \to \infty} \frac{K^t(X \upharpoonright n)}{n}.$$

PRG to Infinite strings



$$\mathcal{K}_{poly}(g(X)) \leq s$$

Pseudorandom generators

1. Generated from a short seed

$$K_t(G(x)) \leq sn + O(1) \quad (s < 1)$$

2. Yet indistinguishable from uniform

Pseudorandom generators

1. Generated from a short seed

$$\mathcal{K}_{poly}(g(X)) \leq s \quad (s < 1)$$

2. Yet indistinguishable from uniform

Pseudorandom generators

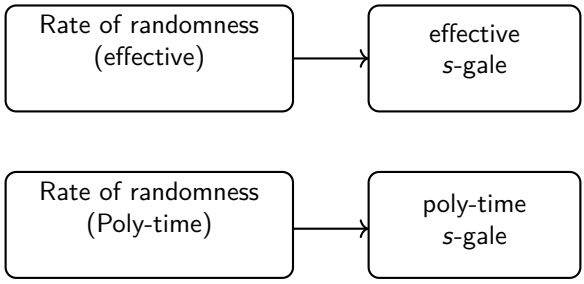
1. Generated from a short seed

$$\mathcal{K}_{poly}(g(X)) \leq s \quad (s < 1)$$

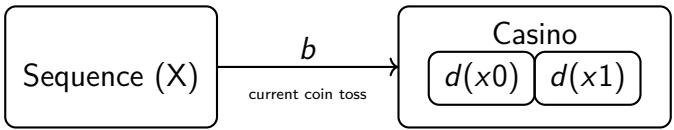
2. Yet indistinguishable from uniform

Question : Poly-time dimension $g(X)$ is high ?

Tests of randomness $\Rightarrow$ s-gales



Impatient Stingy Casino : poly-time s-gale



$$2^s\, d(x) = d(x0) + d(x1) \qquad s \in (0, 1]$$

$d(x)$ runs in time poly($|x|$)

Poly-time dimension

$$\dim_P(X) \;=\; \inf\{\, s \;:\; \exists \text{ poly-time } s\text{-gale } d \text{ that succeeds on } X \,\}$$

least bias needed to win "fast" against X

d succeeds on X iff $\limsup_n d(X \upharpoonright n) = \infty$

Equivalence ?

Hitchcock, Vinodchandran, 2005 :

$$\forall X \in \{0,1\}^\infty, \quad \mathcal{K}_{poly}(X) \leq \dim_P(X).$$

Robustness question of poly-time dimension

$$\forall X \in \{0,1\}^\infty, \quad \mathcal{K}_{poly}(X) \stackrel{?}{=} \dim_P(X).$$

OWF $\implies$ No Equivalence

Nanadakumar, Pulari, A.S, Sarma [2025] :

$$\exists \text{OWF} \implies \exists X \in \{0,1\}^{\infty}, \;\; \mathcal{K}_{poly}(X) \neq \dim_P(X).$$

OWF $\implies$ No Equivalence

$$\exists \text{ OWF} \implies$$

$$\exists \text{“large” collection of } X \in \{0,1\}^\infty, \quad \mathcal{K}_{poly}(X) \neq \dim_P(X).$$

No Equivalence $\implies$ OWF

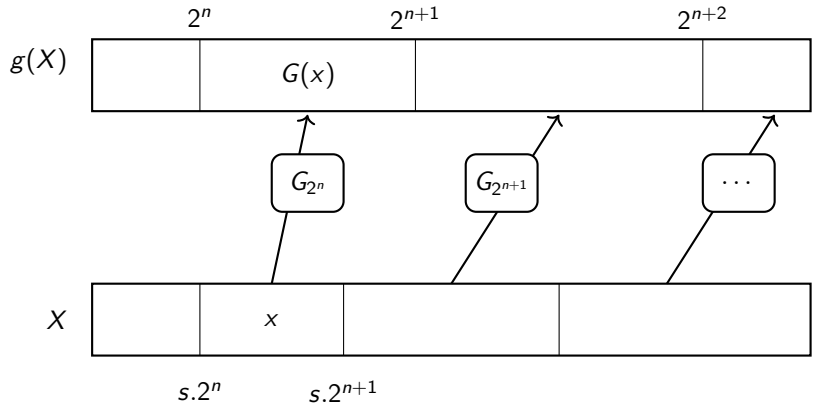
$$\exists \text{“large collection of ”} X \in \{0,1\}^{\infty}, \quad \mathcal{K}_{poly}(X) \neq \dim_P(X).$$

$$\implies \exists \text{ i.o-OWF}$$

No Equivalence

$$\forall X \in \{0,1\}^{\infty},\ \ \mathcal{K}_{poly}(X) = \dim_P(X) \implies \not\exists \text{ PRG}$$

PRG to Infinite strings



$$\mathcal{K}_{poly}(g(X)) \leq s$$

No Equivalence

$$\forall X \in \{0,1\}^\infty, \quad \mathcal{K}_{poly}(X) = \dim_P(X)$$

$$\implies \text{poly-time } s\text{-gale that wins on g(X)}$$

No Equivalence

$$\forall X \in \{0,1\}^{\infty}, \quad \mathcal{K}_{poly}(X) = \dim_P(X)$$

$$\implies \text{poly-time } s\text{-gale that wins on g(X)}$$

$$\cdots\cdots\cdots \implies \exists \text{ poly-time attacker } A \text{ that breaks G}$$

No Equivalence

$$\forall X \in \{0,1\}^{\infty}, \quad \mathcal{K}_{poly}(X) = \dim_P(X)$$

$$\implies \text{poly-time } s\text{-gale that wins on g(X)}$$

$$\cdots\cdots\cdots \implies \not\exists \text{ PRG}$$

Randomness and Compressibility

	Gale		**K.C**
Effective	$\dim(X)$	$=$	$\liminf \frac{K(X\upharpoonright n)}{n}$
PSpace	$\dim_{PSPACE}(X)$	$=$	$\inf_{s\in PSPACE} \liminf \frac{K^s(X\upharpoonright n)}{n}$
Polynomial-time	$\dim_P(X)$	$>$ [1]	$\inf_{t\in poly} \liminf \frac{K^t(X\upharpoonright n)}{n}$

[1] If One-way-functions exist