

On Hierarchies of Randomness Tests

Jan Reimann and Frank Stephan

Universität Heidelberg

National University of Singapore

<http://math.uni-heidelberg.de/logic/reimann/lectures.html>

Randomness and Tests

Informal: Random sets cannot be captured by effective tests succeeding on sets of measure 0 .

Idea of Formalization: Let $\rho(\mathbf{x}) = 2^{-|\mathbf{x}|}$. An effective way to generate a class \mathbf{C} of measure \mathbf{r} is to enumerate a set

$\tilde{\mathbf{C}} = \{\mathbf{x}_0, \mathbf{x}_1, \dots\}$ of strings such that

- $\rho(\tilde{\mathbf{C}}) = \rho(\mathbf{x}_0) + \rho(\mathbf{x}_1) + \rho(\mathbf{x}_2) + \dots = \mathbf{r}$;
- $\mathbf{C} = \{\mathbf{A} : \exists n (\mathbf{x}_n \sqsubset \mathbf{A})\}$.

Martin-Löf Test: \mathbf{A} is covered by a test given by a uniformly r.e. family $\mathbf{V}_0, \mathbf{V}_1, \dots$ such that every \mathbf{V}_i contains a prefix of \mathbf{A} and $\rho(\mathbf{V}_i) = < 2^{-i}$.

Solovay Test: \mathbf{A} is covered by a test given by an r.e. set \mathbf{W} of strings such that $\rho(\mathbf{W}) < \infty$ and \mathbf{W} contains infinitely many prefixes of \mathbf{A} .

Kolmogorov Complexity

General idea: Amount of information needed to describe effectively a string.

Prefix-Free Complexity: $H(x) = \min\{|\mathbf{p}| : \mathbf{U}(\mathbf{p}) = x\}$.

Based on universal prefix-free machine \mathbf{U}

Prefix-free: If $\mathbf{p} \prec \mathbf{q}$ and $\mathbf{U}(\mathbf{p})$ defined then $\mathbf{U}(\mathbf{q})$ undefined.

Universal: Machine which cannot be improved much. For every further prefix-free machine \mathbf{V} the best program for any input can only be constantly shorter as the corresponding program for \mathbf{U} . That is, \mathbf{U} satisfies the formula

$\forall \mathbf{V} \exists c \forall \mathbf{p} \exists \mathbf{q} [\mathbf{V}(\mathbf{p}) \text{ defined} \Rightarrow \mathbf{U}(\mathbf{q}) = \mathbf{V}(\mathbf{p}) \wedge |\mathbf{q}| \leq |\mathbf{p}| + c]$.

Remark: The original version of Kolmogorov complexity as introduced by Kolmogorov and Solomonoff does not request the machine to be prefix-free. Both versions are widely studied.

Characterizing Randomness

Theorem [Martin-Löf, Schnorr, Solovay]

A set \mathbf{A} is random iff one of the following equivalent conditions holds:

- \mathbf{A} is not covered by any Martin-Löf test;
- \mathbf{A} is not covered by any Solovay test;
- $\forall^\infty n (\mathbf{H}(\mathbf{A}(0)\mathbf{A}(1) \dots \mathbf{A}(n)) \geq n + 1)$.

Characterizations based on Lebesgue measure and its properties. Tadaki as well as Calude, Staiger and Terwijn propose to use other measure functions ρ in order to investigate various degrees of randomness.

- What about $\rho(\mathbf{x}) = 2^{-r \cdot |\mathbf{x}|}$ for some r strictly between 0 and 1 ? Should other measure functions be considered?
- How to reformulate the randomness tests?
- Which connections are between these tests?

Measure-Functions

Measure Function

All: $\exists \mathbf{p} < \mathbf{1} \forall \mathbf{x}, \mathbf{a} ((\rho(\mathbf{x}\mathbf{a}) < \mathbf{p} \cdot \rho(\mathbf{x})) \wedge (\rho(\mathbf{x}) \leq \rho(\mathbf{x}\mathbf{0}) + \rho(\mathbf{x}\mathbf{1})))$.

Unbounded: $\exists \mathbf{q} < \mathbf{1} \forall \mathbf{x} (\rho(\mathbf{x}) < \mathbf{q} \cdot (\rho(\mathbf{x}\mathbf{0}) + \rho(\mathbf{x}\mathbf{1})))$.

Length-Independent: $\forall \mathbf{x}, \mathbf{y} (|\mathbf{x}| = |\mathbf{y}| \Rightarrow \rho(\mathbf{x}) = \rho(\mathbf{y}))$.

One can adapt the various characterizations for randomness to the measure function ρ .

Question [Calude, Staiger and Terwijn 2005]

If $\rho(\mathbf{x}) = 2^{-\mathbf{r} \cdot |\mathbf{x}|}$ for some $\mathbf{r} < \mathbf{1}$, do the various notions of ρ -randomness coincide?

Calude, Staiger and Terwijn gave several formalizations and showed that they coincide with three notions for which it remained open whether they are equal.

Notions of ρ -Randomness

A is Martin-Löf ρ -random if there is no uniformly r.e. family $\mathbf{V}_0, \mathbf{V}_1, \dots$ of sets such that, for all i , \mathbf{V}_i contains a prefix of **A** and $\rho(\mathbf{V}_i) < 2^{-i}$.

A is strongly Martin-Löf ρ -random if there is no uniformly r.e. family $\mathbf{V}_0, \mathbf{V}_1, \dots$ of sets such that, for all i , \mathbf{V}_i contains a prefix of **A** and $\rho(\mathbf{W}) < 2^{-i}$ for every prefix-free $\mathbf{W} \subseteq \mathbf{V}_i$.

A is Solovay ρ -random if there is no r.e. set \mathbf{W} of strings containing infinitely many prefixes of **A** with $\rho(\mathbf{W}) < \infty$.

A is weakly Chaitin ρ -random if

$$\exists c \forall n (\rho(\mathbf{A}(0)\mathbf{A}(1) \dots \mathbf{A}(n)) \geq 2^{-H(\mathbf{A}(0)\mathbf{A}(1) \dots \mathbf{A}(n)) - c}).$$

A is strongly Chaitin ρ -random if

$$\forall c \forall^\infty n (\rho(\mathbf{A}(0)\mathbf{A}(1) \dots \mathbf{A}(n)) \geq 2^{c - H(\mathbf{A}(0)\mathbf{A}(1) \dots \mathbf{A}(n))}).$$

Solovay \Leftrightarrow Strong Chaitin

Theorem [Calude, Staiger, Terwijn 2005]

Every Solovay ρ -random set is strongly Chaitin ρ -random.

Proof: Let \mathbf{A} be not strongly Chaitin ρ -random. There is constant \mathbf{c} such that

$$\exists^\infty \mathbf{n} (\rho(\mathbf{A}(0)\mathbf{A}(1)\dots\mathbf{A}(\mathbf{n})) < 2^{\mathbf{c}-\mathbf{H}(\mathbf{A}(0)\mathbf{A}(1)\dots\mathbf{A}(\mathbf{n}))}).$$

Let $\mathbf{W} = \{\mathbf{x} : \rho(\mathbf{x}) < 2^{\mathbf{c}-\mathbf{H}(\mathbf{x})}\}$. Note that $\rho(\mathbf{W}) < 2^{\mathbf{c}}$.

\mathbf{W} witnesses that \mathbf{A} is not Solovay ρ -random.

Theorem [Calude, Staiger, Terwijn 2005]

Every strongly Chaitin ρ -random set is Solovay ρ -random.

Idea: Given a Solovay ρ -test \mathbf{W} covering \mathbf{A} , one can use the Kraft-Chaitin theorem to show that there is a constant \mathbf{c} such that every $\mathbf{x} \in \mathbf{W}$ satisfies $\rho(\mathbf{x}) < 2^{\mathbf{c}-\mathbf{H}(\mathbf{x})}$.

Martin-Löf \Leftrightarrow Weak Chaitin

Theorem [Tadaki 2002 for $\rho(\mathbf{x}) = 2^{-r \cdot |\mathbf{x}|}$; Reimann 2004]
If ρ is unbounded and length-independent then the Martin-Löf ρ -random sets coincide with the weakly Chaitin ρ -random sets.

One Direction

If \mathbf{A} is not weakly Chaitin random then \mathbf{A} is covered by the Martin-Löf ρ -test

$$\mathbf{V}_n = \{\mathbf{x} : \rho(\mathbf{x}) < 2^{-n-H(\mathbf{x})}\}$$

where, for all n , $\rho(\mathbf{V}_n) < 2^{-n}$ and \mathbf{V}_n contains a prefix of \mathbf{A} .

Conjecture

Equivalence holds also for all measure-functions.

Weak Chaitin $\not\Rightarrow$ Strong Chaitin

Theorem [Cai, Hartmanis 1994, Lutz 2001 for $\rho(\mathbf{x}) = 2^{-r \cdot |\mathbf{x}|}$]
If ρ is unbounded then there is a set \mathbf{A} which is weakly Chaitin ρ -random but not strongly Chaitin ρ -random.

Proof

There is \mathbf{c} such that for all \mathbf{x} there are $\mathbf{y}, \mathbf{z} \in \{0, 1\}^{\mathbf{c}}$ with

- $\mathbf{H}(\mathbf{xy}) - \log(\rho(\mathbf{xy})) > \mathbf{H}(\mathbf{x}) - \log(\rho(\mathbf{x})) + 1$;
- $\mathbf{H}(\mathbf{xz}) - \log(\rho(\mathbf{xz})) < \mathbf{H}(\mathbf{x}) - \log(\rho(\mathbf{x})) - 1$.

So one can build by finite extension an infinite sequence \mathbf{A} such that $\mathbf{H}(\mathbf{x}) - \log(\rho(\mathbf{x}))$ is almost the same for all prefixes of \mathbf{A} . This set \mathbf{A} is weakly Chaitin ρ -random but not strongly Chaitin ρ -random.

This construction needs unboundedness as the example of the standard measure-function $\rho(\mathbf{x}) = 2^{-|\mathbf{x}|}$ shows.

Solovay \Rightarrow Martin-Löf

Proposition

Every Solovay ρ -random set is Martin-Löf ρ -random.

Idea

An array defining a Martin-Löf ρ -test covering \mathbf{A} can also be viewed as a Solovay ρ -test covering \mathbf{A} .

Theorem

If ρ is unbounded and length-independent then there is a set \mathbf{A} which is Martin-Löf ρ -random but not Solovay ρ -random.

Proof

Under the constraints given in the theorem the notion Martin-Löf ρ -random equals to weakly Chaitin ρ -random and the notion Solovay ρ -random equals to strong Chaitin ρ -random. Furthermore, the two Chaitin ρ -randomness notions are different.

Strongly Martin-Löf \Rightarrow Solovay

Theorem

Every strongly Martin-Löf ρ -random set is Solovay ρ -random.

Construction: Let $\mathbf{W}_x^+ = \{\mathbf{xy} : |\mathbf{y}| > \mathbf{0} \wedge \mathbf{xy} \in \mathbf{W}\}$.

If $\forall n \exists \mathbf{x} \sqsubset \mathbf{A} (\mathbf{x} \in \mathbf{W} \wedge \rho(\mathbf{x}) \cdot 2^n < \rho(\mathbf{W}_x^+))$

Then $\mathbf{V}_n = \{\mathbf{x} \in \mathbf{W} : \rho(\mathbf{x}) \cdot 2^n < \rho(\mathbf{W}_x^+)\}$

Else let \mathbf{q} be a rational such that

- $\exists^\infty \mathbf{x} \sqsubset \mathbf{A} (\rho(\mathbf{x}) < \mathbf{q} \cdot \rho(\mathbf{W}_x^+))$;
- $\exists^\infty \mathbf{x} \sqsubset \mathbf{A} (\rho(\mathbf{x}) < (\mathbf{q} + \mathbf{0.5}) \cdot \rho(\mathbf{W}_x^+))$.

One enumerates a subset \mathbf{T} of \mathbf{W} which satisfies the first condition for infinitely many prefixes of \mathbf{A} and the second for all \mathbf{x} . Let

$\mathbf{S} = \{\mathbf{x} \in \mathbf{T} : \rho(\mathbf{x}) < \mathbf{q} \cdot \rho(\mathbf{T}_x^+)\}$ and

$$\mathbf{V}_n = \{\mathbf{x} \in \mathbf{T} : |\{\mathbf{y} \sqsubseteq \mathbf{x} : \mathbf{y} \in \mathbf{T}\}| > \mathbf{m}_n\}$$

for a suitable \mathbf{m}_n computed from \mathbf{n} .

Solovay $\not\Rightarrow$ Strong Martin-Löf

Theorem

Let ρ be length-independent and unbounded. \exists Solovay ρ -random set \mathbf{A} which is not strongly Martin-Löf ρ -random.

Idea: Let $\mathbf{r}(\mathbf{x}) = -\log(\rho(\mathbf{x}))$ and $\mathbf{l}_0, \mathbf{l}_1, \dots$ be a recursive sequence of disjoint intervals such that

$$\forall \mathbf{i} \exists \mathbf{j} \in \mathbf{l}_i \forall \mathbf{k} (|\{\mathbf{x} \in \{0, 1\}^{\mathbf{j}} : \mathbf{H}(\mathbf{x}) \leq \mathbf{k}\}| < 2^{\mathbf{k}-2\mathbf{i}}).$$

Then construct a set \mathbf{A} such that, up to a constant \mathbf{c} ,

$$\forall \mathbf{i} \forall \mathbf{j} \in \mathbf{l}_i (\mathbf{H}(\mathbf{A}(0)\mathbf{A}(1) \dots \mathbf{A}(\mathbf{j} - 1))) = \mathbf{r}(0^{\mathbf{j}}) + \mathbf{i}).$$

By construction \mathbf{A} is Solovay ρ -random. Let

$$\mathbf{W}_i = \{\mathbf{x} \in \{0, 1\}^{\max(\mathbf{l}_i + \mathbf{c})} : \forall \mathbf{y} \sqsubseteq \mathbf{x} (\mathbf{H}(\mathbf{y}) \leq \mathbf{r}(\mathbf{y}) + \mathbf{i} + 2\mathbf{c})\}.$$

Although $\mathbf{W}_0, \mathbf{W}_1, \dots$ is not yet a strong Martin-Löf ρ -test, one can modify it to one which still covers \mathbf{A} .

Summary

For an unbounded length-independent measure-function ρ , the hierarchy of randomness-notions has three levels:

- Strongly Martin-Löf ρ -random;
- Solovay ρ -random, strongly Chaitin ρ -random;
- Martin-Löf ρ -random, weakly Chaitin ρ -random.

The separation of the second and third levels and the equivalence of the two notions on the third level is up to now only proven for length-independent measure functions.

All separation results need unbounded measure functions.