# 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 $\mathbf{0}$.

Idea of Formalization: Let $\rho(\mathbf{x}) = \mathbf{2}^{-|\mathbf{x}|}$. An effective way to generate a class $\mathbf{C}$ of measure $\mathbf{r}$ is to enumerate a set $\tilde{\mathbf{C}} = \{\mathbf{x_0}, \mathbf{x_1}, \ldots\}$ of strings such that

- $\rho(\tilde{\mathbf{C}}) = \rho(\mathbf{x_0}) + \rho(\mathbf{x_1}) + \rho(\mathbf{x_2}) + \ldots = \mathbf{r}$;
- $\mathbf{C} = \{\mathbf{A} : \exists \mathbf{n}\, (\mathbf{x_n} \sqsubset \mathbf{A})\}$.

Martin-Löf Test: $\mathbf{A}$ is covered by a test given by a uniformly r.e. family $\mathbf{V_0}, \mathbf{V_1}, \ldots$ such that every $\mathbf{V_i}$ contains a prefix of $\mathbf{A}$ and $\rho(\mathbf{V_i}) =< \mathbf{2}^{-\mathbf{i}}$.

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

Based on universal prefix-free machine U

Prefix-free: If $\mathbf{p} \prec \mathbf{q}$ and $\mathbf{U(p)}$ defined then $\mathbf{U(q)}$ 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 corres- ponding program for $\mathbf{U}$. That is, $\mathbf{U}$ satisfies the formula
$\forall \mathbf{V} \exists \mathbf{c} \forall \mathbf{p} \exists \mathbf{q} \, [\mathbf{V(p)} \text{ defined } \Rightarrow \mathbf{U(q) = V(p)} \wedge |\mathbf{q}| \leq |\mathbf{p}| + \mathbf{c}]$.

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;
- $\forall^\infty \mathbf{n}\, (\mathbf{H}(\mathbf{A}(\mathbf{0})\mathbf{A}(\mathbf{1}) \ldots \mathbf{A}(\mathbf{n})) \geq \mathbf{n} + \mathbf{1})$.

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

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

# Measure-Functions

Measure Function
All: $\exists \mathbf{p} < \mathbf{1}\, \forall \mathbf{x}, \mathbf{a}\, ((\rho(\mathbf{xa}) < \mathbf{p} \cdot \rho(\mathbf{x})) \wedge (\rho(\mathbf{x}) \leq \rho(\mathbf{x0}) + \rho(\mathbf{x1})))$.
Unbounded: $\exists \mathbf{q} < \mathbf{1}\, \forall \mathbf{x}\, (\rho(\mathbf{x}) < \mathbf{q} \cdot (\rho(\mathbf{x0}) + \rho(\mathbf{x1})))$.
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 $\rho$.

Question [Calude, Staiger and Terwijn 2005]
If $\rho(\mathbf{x}) = \mathbf{2}^{-\mathbf{r} \cdot |\mathbf{x}|}$ for some $\mathbf{r} < \mathbf{1}$, do the various notions of $\rho$-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 $\rho$-Randomness

**A** is Martin-Löf $\rho$-random if there is no uniformly r.e. family $\mathbf{V_0}, \mathbf{V_1}, \ldots$ of sets such that, for all $\mathbf{i}$, $\mathbf{V_i}$ contains a prefix of **A** and $\rho(\mathbf{V_i}) < \mathbf{2^{-i}}$.

**A** is strongly Martin-Löf $\rho$-random if there is no uniformly r.e. family $\mathbf{V_0}, \mathbf{V_1}, \ldots$ of sets such that, for all $\mathbf{i}$, $\mathbf{V_i}$ contains a prefix of **A** and $\rho(\mathbf{W}) < \mathbf{2^{-i}}$ for every prefix-free $\mathbf{W} \subseteq \mathbf{V_i}$.

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

**A** is weakly Chaitin $\rho$-random if

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

**A** is strongly Chaitin $\rho$-random if

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

# Solovay $\Leftrightarrow$ Strong Chaitin

Theorem [Calude, Staiger, Terwijn 2005]
Every Solovay $\rho$-random set is strongly Chaitin $\rho$-random.

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

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

Let $\mathbf{W} = \{\mathbf{x} : \rho(\mathbf{x}) < \mathbf{2^{c-H(x)}}\}$. Note that $\rho(\mathbf{W}) < \mathbf{2^c}$.
$\mathbf{W}$ witnesses that $\mathbf{A}$ is not Solovay $\rho$-random.

Theorem [Calude, Staiger, Terwijn 2005]
Every strongly Chaitin $\rho$-random set is Solovay $\rho$-random.

Idea: Given a Solovay $\rho$-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 $\rho(\mathbf{x}) < \mathbf{2^{c-H(x)}}$.

# Martin-Löf $\Leftrightarrow$ Weak Chaitin

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

One Direction
If $\mathbf{A}$ is not weakly Chaitin random then $\mathbf{A}$ is covered by the Martin-Löf $\rho$-test

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

where, for all $\mathbf{n}$, $\rho(\mathbf{V_n}) < \mathbf{2}^{-\mathbf{n}}$ 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 $\rho(\mathbf{x}) = \mathbf{2}^{-\mathbf{r}\cdot|\mathbf{x}|}$]
If $\rho$ is unbounded then there is a set $\mathbf{A}$ which is weakly Chaitin $\rho$-random but not strongly Chaitin $\rho$-random.

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

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

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

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

# Solovay $\Rightarrow$ Martin-Löf

**Proposition**

Every Solovay $\rho$-random set is Martin-Löf $\rho$-random.

**Idea**

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

**Theorem**

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

**Proof**

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

# Strongly Martin-Löf $\Rightarrow$ Solovay

**Theorem**

Every strongly Martin-Löf $\rho$-random set is Solovay $\rho$-random.

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

If $\forall n \exists x \sqsubset A\, (x \in W \wedge \rho(x) \cdot 2^n < \rho(W_x^+))$

Then $V_n = \{x \in W : \rho(x) \cdot 2^n < \rho(W_x^+)\}$

Else let $q$ be a rational such that

- $\exists^\infty x \sqsubset A\, (\rho(x) < q \cdot \rho(W_x^+))$;
- $\exists^\infty x \sqsubset A\, (\rho(x) < (q + 0.5) \cdot \rho(W_x^+))$.

One enumerates a subset $T$ of $W$ which satisfies the first condition for infinitely many prefixes of $A$ and the second for all $x$. Let $S = \{x \in T : \rho(x) < q \cdot \rho(T_x^+)\}$ and

$$V_n = \{x \in T : |\{y \sqsubseteq x : y \in T\}| > m_n\}$$

for a suitable $m_n$ computed from $n$.

# Solovay $\not\Rightarrow$ Strong Martin-Löf

Theorem

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

Idea: Let $\mathbf{r(x) = -log(\rho(x))}$ and $\mathbf{I_0, I_1, \ldots}$ be a recursive sequence of disjoint intervals such that

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

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

$$\forall \mathbf{i} \forall \mathbf{j} \in \mathbf{I_i}\, (\mathbf{H(A(0)A(1)\ldots A(j-1)) = r(0^j) + i}).$$

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

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

Although $\mathbf{W_0, W_1, \ldots}$ is not yet a strong Martin-Löf $\rho$-test, one can modify it to one which still covers $\mathbf{A}$.

# Summary

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

- Strongly Martin-Löf $\rho$-random;
- Solovay $\rho$-random, strongly Chaitin $\rho$-random;
- Martin-Löf $\rho$-random, weakly Chaitin $\rho$-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.