The Metamathematics of Algorithmic Randomness

Jan Reimann
(joint work with Theodore Slaman)

Department of Mathematics
University of California, Berkeley

Logic Colloquium 2006, Nijmegen
Question

For which reals $X \in 2^\omega$ does there exist (a representation of) a measure $\mu$ such that $X$ is random for $\mu$?
We want to generalize Martin-Löf randomness to arbitrary measures. For this, we have to access measures as oracles.

- In Cantor space we can simply code the rational approximations to a measure in a real.
- More general, if a space $X$ is Polish, so is the space $\mathcal{M}(X)$ of all probability measures on $X$ (under the weak topology). Also, if $X$ is compact metrizable, so is $\mathcal{M}(X)$.

Note that there are various ways to represent a measure: Cauchy sequences, list of basic open balls it is contained in, etc.

- There might not be a least representation in terms of Turing-degree.
Definition

Let $m$ be a representation of some $\mu \in \mathcal{M}(2^{<\omega})$, and let $n \geq 1$.

- An $n$-Martin-Löf test for $m$ is a sequence $(V_n)_{n \in \mathbb{N}}$ of subsets of $2^{<\omega}$ such that $(V_n)$ is uniformly r.e. in $m^{(n-1)}$ and for each $n$,

$$\sum_{\sigma \in V_n} \mu(N_\sigma) \leq 2^{-n}.$$

- A real $X$ is $n$-random for $m$ if for every $n$-Martin-Löf test for $m$,

$$X \notin \bigcap_{k} \bigcup_{\sigma \in V_k} N_\sigma.$$
Non-Trivial Randomness

Note that every real is trivially random with respect to some $\mu$ if it is an atom of $\mu$.

- We are interested in the case when a real is non-trivially random.

**Theorem (Reimann and Slaman)**

*For any real $X$, there exists (a representation of) a measure $\mu$ such that $\mu(\{X\}) \neq 0$ and $X$ is 1-random for $\mu$ if and only if $X$ is not recursive.*

In the proof there is no control over the measure obtained.

- Atoms cannot be avoided.
- Uses a special (though natural) representation of $\mathcal{M}(2^\omega)$ as a particular $\Pi^0_1$ class.
Non-Trivial Randomness

Features needed in the proof:

▶ **Conservation of randomness:**
  ▶ If \( f : 2^\omega \rightarrow 2^\omega \) is continuous, \( \mu \) a measure, then \( \mu_f(A) := \mu(f^{-1}(A)) \) defines the image measure.
  ▶ If \( f \) is effective and \( X \) is random for \( \mu \), \( f(X) \) is random for \( \mu_f \).

▶ **Randomness of cones:**
  ▶ Kucera’s coding argument shows that every degree above \( \emptyset' \) is random.
  ▶ Relativize this using the Posner-Robinson Theorem.
Neutral Measure

A similar result can be obtained by using a neutral measure, relative to which every real looks random.

Theorem (Levin; Gacs)

There exists a measure $\mu$ such that for every $X$, $t_\mu(X) \leq 1$, where $t_\mu(X)$ is a universal test for randomness for $\mu$.

- The proof uses the combinatorial Sperner Lemma.
- Works only for compact spaces.
Continuous Randomness

In the following, we will concentrate on continuous, i.e. non-atomic measures.

- For these, the transformation of measures and randomness (and with it the representation of the measure) is particularly well-behaved.

- **Classical result:** For every continuous measure $\mu$ there is a Borel isomorphism $f$ of $2^\omega$ such that $\mu = \lambda_f$, $\lambda$ being Lebesgue measure.
Theorem (Levin; Kautz; Reimann and Slaman)

Let $X$ be a real. The following are equivalent.

(i) $X$ is truth-table equivalent to a Martin-Löf random real.

(ii) $X$ is random for a continuous recursive measure.

(iii) $X$ is random for a continuous dyadic recursive measure.

(iv) There exists a recursive functional $\Phi$ which is an order-preserving homeomorphism of $2^\omega$ such that $\Phi(X)$ is Martin-Löf random.

Hence we can define (continuous) randomness degree-theoretically.
The Class NCR

Question

Which level of logical complexity guarantees continuous randomness?

Let $\text{NCR}_n$ be the set of all reals which are not $n$-random relative to any continuous measure.

- **Kjos-Hanssen and Montalban**: Every member of a countable $\Pi^0_1$ class is contained in $\text{NCR}_1$. (It follows that elements of $\text{NCR}_1$ can be found at arbitrary high levels of the hyperarithmetical hierarchy.)

- **Reimann and Slaman**: $\text{NCR}_1 \subseteq \Delta^1_1$.

The proofs are arguments tailored for $n = 1$ and do not carry over to higher levels of randomness.
The Class NCR
Examples of higher order

Theorem

*Kleene’s $\emptyset$ is an element of NCR$_3$.*

Based on this, one can use the theory of *jump operators* (Jockusch ans Shore) to obtain a whole class of examples.

Proof:

- Tree representation of $\emptyset$:

  \[ \emptyset = \{ e : \text{the $e$th recursive tree } T_e \subseteq \omega^{<\omega} \text{ is well-founded} \}. \]

- Suppose $\emptyset$ is 3-random for some $\mu$.

- We want to use *domination properties* of random reals.
The Class NCR
Examples of higher order

- **Well-known** (Kurtz and others): If $X$ is $n$-random for $\mu$, $n > 1$, then every function $f \leq_T X$ is dominated by a function recursive in $\mu'$.

- Therefore, $\mu'$ computes a uniform family $\{g_e\}$ of functions dominating the leftmost infinite path of $T_e$.

- Use **compactness** to infer: For every $e$, the following are equivalent.
  
  (i) $T_e$ is well-founded.
  (ii) The subtree of $T_e$ to the left of $g_e$ is finite.

- The latter condition is $\Pi^0_1(\mu')$, hence $\emptyset$ is $\Pi^0_2(\mu)$.

- But this is impossible if $\emptyset$ is 3-random for $\mu$. 
Lower Bounds for Continuous Randomness

In general, can we give a distinct bound on $\text{NCR}_n$ like in the case $n = 1$?

- There is some evidence that $\text{NCR}_n$ grows very quickly with $n$.
- Can we give an upper bound?

**Theorem (Slaman)**

For all $n$, $\text{NCR}_n$ is countable.
NCR\(_n\) is Countable

Proof:

- Show that the complement of NCR\(_n\) contains an upper Turing cone.
  - Show that the complement of NCR\(_n\) contains a Turing invariant and cofinal Borel set. We can use the set of all \(Y\) that are Turing equivalent to some \(Z \oplus R\), where \(R\) is \((n + 1)\)-random relative to \(Z\).
  - Use Martin’s result on Borel Turing sets to infer that the complement of NCR\(_n\) contains a cone.

- Go on to show that the elements of NCR\(_n\) are definable at a rather low level of the constructible universe.
  - NCR\(_n\) \(\subseteq L_{\beta_n}\), where \(\beta_n\) is the least ordinal such that
    \[L_{\beta_n} \models ZFC^- + \text{there exist } n \text{ many iterates of the power set of } \omega,\]
    where \(ZFC^-\) is Zermelo-Fraenkel set theory without the Power Set Axiom.
  - Note that \(L_{\beta_n}\) is countable.
Question

Do we need to use metamathematical methods to prove the countability of $\text{NCR}_n$?

We make fundamental use of Borel determinacy; this suggests to analyze the metamathematics in this context.
The necessity of iterates of the power set is known from a famous result by Friedman.

- Martin’s proof of Borel determinacy starts with a description of a Borel game and produces a winning strategy for one of the players.
- The more complicated the game is in the Borel hierarchy, the more iterates of the power set of the continuum are used in producing the strategy.

**Theorem (Friedman)**

\[ \text{ZFC} \not\models \forall \Sigma_5^0 \text{-games on countable trees are determined.} \]

Martin later improved this to \( \Sigma_4^0 \).
Friedman’s Result on Borel Determinacy

Inductively one can infer from Friedman’s result that in order to prove full Borel determinacy, a result about sets of reals, one needs infinitely many iterates of the power set of the continuum.

- The proof works by showing that there is a model of $\text{ZFC}^-$ for which $\Sigma^0_4$-determinacy does not hold.
- This model is $L_{\beta_0}$.
We can work along similar lines to obtain a similar result concerning the countability of \( \text{NCR}_n \).

**Theorem**

For every \( k \), the statement

\[
\text{For every } n, \text{NCR}_n \text{ is countable.}
\]

cannot be proven in \( \text{ZFC}^− \) + \text{there exists } k \text{ many iterates of the power set of } \omega.

The proof (for \( k = 0 \)) shows that there is an \( n \) such that \( \text{NCR}_n \) is cofinal in the Turing degrees of \( L_{\beta_0} \). Hence, \( \text{NCR}_n \) is not countable in \( L_{\beta_0} \).