Randomness notions and reverse mathematics

Paul Shafer
University of Leeds
p.e.shafer@leeds.ac.uk
http://www1.maths.leeds.ac.uk/~matpsh/

Computability Theory and Applications Online Seminar
Midwest Computability Seminar
November 10, 2020

Joint work with André Nies.

Algorithmic randomness

The basic idea:
Let $X, Z \in 2^{\mathbb{N}}$ (thought of as infinite bit sequences).

We say that X is **random** relative to Z if Z cannot be used to describe/predict/compress the bits of X.

Different formalizations of this idea yield different randomness notions.

Today:
Explore randomness notions as set-existence axioms:

"For every set Z, there is a set X that is random relative to Z."

Questions that one might ask:

- Can randomness axioms be used to prove classical mathematical theorems?
- **Our focus**: How do randomness axioms relate to each other?

For example:

(Don't worry about what the randomness notions mean for now.)

Computable randomness (CR) versus **Schnorr randomness** (SR):

- Every computably random set is Schnorr random.
- **Not** every Schnorr random set is computably random.
- Nevertheless, every Schnorr random set **computes** a computably random set (which follows from Nies, Stephan, and Terwijn).
- **As randomness axioms**: $\mathsf{RCA}_0 \vdash \mathsf{SR} \Leftrightarrow \mathsf{CR}$.

Martin-Löf randomness (MLR) versus **computable randomness** (CR):

- Every Martin-Löf random set is computably random.
- **Not** every computably random set is Martin-Löf random.
- **As randomness axioms**:
  - $\mathsf{RCA}_0 + \mathsf{MLR} \vdash \mathsf{CR}$.
  - $\mathsf{RCA}_0 + \mathsf{CR} \nvdash \mathsf{MLR}$.
  - In fact, $\mathsf{RCA}_0 + \mathsf{CR} \nvdash \mathsf{DNR}$.

Reverse mathematics reminders

Formally we work in **second-order arithmetic**, which means the objects are **natural numbers** and **sets of natural numbers**.

We can make sense of a lot of other objects via **coding**, such as:

Trees   Reals numbers   The topology on $\mathbb{R}$ Continuous functions   etc.

Today's **axiom systems** are:

RCA_0: Sets computable from existing sets exist (formally, Δ^0_1 comprehension). Induction is restricted to Σ^0_1 formulas (formally, $\mathsf{I}\Sigma^0_1$).

WKL_0: Add to RCA_0 the statement "every infinite subtree of $2^{<\mathbb{N}}$ has an infinite path."

ACA_0: Every arithmetical formula defines a set.

Martin-Löf tests and Martin-Löf randomness

Recall: For a set $U \subseteq 2^{<\mathbb{N}}$,

$$[\![U]\!] = \bigcup_{\sigma \in U} [\![\sigma]\!] = \text{the open set coded by } U.$$

A **Martin-Löf test** relative to $Z \in 2^{\mathbb{N}}$ is a uniformly Z-r.e. sequence

$$U_0, U_1, U_2, \dots$$

of subsets of $2^{<\mathbb{N}}$ such that for every $n \in \mathbb{N}$:

$$\mu([\![U_n]\!]) \leq 2^{-n}.$$

Think of a ML-test relative to Z as describing an **effective null set** relative to Z.

$X \in 2^{\mathbb{N}}$ **passes** the ML-test $(U_n : n \in \mathbb{N})$ if

$$X \notin \bigcap_{n \in \mathbb{N}} [\![U_n]\!].$$

X is **Martin-Löf random** relative to Z if X **passes every ML-test** relative to Z.

ML-randomness as a set-existence axiom

It is reasonably straightforward to phrase

"X is ML-random relative to Z"

in second-order arithmetic.

Definition

MLR is the statement

$$\forall Z \, \exists X \, (X \text{ is ML-random relative to } Z).$$

Can MLR be used as an axiom to prove interesting mathematical theorems?

MLR and König's lemma

Recall:
$T \subseteq 2^{<\mathbb{N}}$ is a **tree** if it is closed under initial segments:

$$\forall \sigma\, \forall \tau\, (\sigma \in T \wedge \tau \sqsubseteq \sigma \to \tau \in T).$$

Tree T has **positive measure** if there is a rational $q > 0$ such that for all n

$$\frac{\big|\{\sigma \in T : |\sigma| = n\}\big|}{2^n} \geq q.$$

Weak weak König's lemma (WWKL) is the statement "every subtree of $2^{<\mathbb{N}}$ of positive measure has an infinite path."

Theorem (Essentially Kučera):
$\mathsf{RCA}_0 \vdash \mathsf{MLR} \Leftrightarrow \mathsf{WWKL}$.

Theorem (Yu and Simpson):
$\mathsf{RCA}_0 + \mathsf{MLR}$ is strictly between RCA_0 and WKL_0.

Mathematical consequences of MLR

The following are all equivalent to MLR over RCA_0:

- Every Borel measure on a compact Polish space is countably additive. (Yu and Simpson)
- Versions of the Vitali covering theorem. (Brown, Giusto, and Simpson)
- A version of the monotone convergence theorem for Borel measures on compact Polish spaces. (Yu)
- Every continuous $f\colon [0,1] \to \mathbb{R}$ of bounded variation is differentiable at some point. (Nies, Triplett, and Yokoyama)
- Every continuous $f\colon [0,1] \to \mathbb{R}$ of bounded variation is differentiable almost everywhere. (Nies, Triplett, and Yokoyama)

Stronger randomness notions

Recall: X is ML-random relative to Z if X passes every ML-test $(U_n : n \in \mathbb{N})$ relative to Z.

- $(U_n : n \in \mathbb{N})$ is uniformly Z-r.e. with $\mu([\![U_n]\!]) \leq 2^{-n}$.
- X passes $(U_n : n \in \mathbb{N})$ if $X \notin \bigcap_{n \in \mathbb{N}} [\![U_n]\!]$.

Stronger randomness notions are defined by allowing **more tests** which capture **more sets** and hence leave **fewer randoms**.

That is, if there are **more tests**, then it is **harder to pass all tests**.

Definition

A **weak 2-test** relative to Z is like a ML-test relative to Z, except we only require

$$\lim_{n \to \infty} \mu([\![U_n]\!]) = 0$$

instead of $\forall n \, (\mu([\![U_n]\!]) \leq 2^{-n})$.

Weak 2-randomness

A **weak 2-test** relative to Z is a uniformly Z-r.e. sequence $(U_n : n \in \mathbb{N})$ such that $\lim_{n\to\infty} \mu(\llbracket U_n \rrbracket) = 0$.

X is **weakly 2-random** relative to Z if X passes every weak 2-test relative to Z.

Definition

W2R is the statement

$$\forall Z\, \exists X\, (X \text{ is weakly 2-random relative to } Z).$$

2-randomness

Basic idea:
X is 2-**random** relative to Z if X is ML-random relative to Z'.

This definition works fine in ordinary math, but it's a problem over RCA_0 because the statement

"for all sets Z, the set Z' exists"

is equivalent to ACA_0 over RCA_0.

We want to say "X is 2-random relative to Z" in a way that does **not** imply that Z' is a set.

This can be done by letting the components of a test be $\Sigma^{0,Z}_2$ classes instead of $\Sigma^{0,Z'}_1$ classes.

Formalized 2-randomness

If $T \subseteq 2^{<\mathbb{N}}$ is a tree, let $[T]$ denote the class of paths through T.

For $q \in \mathbb{Q}$, define $\mu([T]) \leq q$ if there is an n such that

$$\frac{\left|\{\sigma \in T : |\sigma| = n\}\right|}{2^n} \leq q.$$

Let $Z \in 2^{\mathbb{N}}$.

- A code for a $\Sigma_2^{0,Z}$ class $\mathscr{W}$ is a sequence of trees $(T_n : n \in \mathbb{N}) \leq_{\mathrm{T}} Z$ such that $T_0 \subseteq T_1 \subseteq T_2 \subseteq \cdots$.
- Define $X \in \mathscr{W}$ if $\exists n\left(X \in [T_n]\right)$.
- For $q \in \mathbb{Q}$, define $\mu(\mathscr{W}) \leq q$ if $\forall n\left([T_n] \leq q\right)$.
- A uniform sequence of $\Sigma_2^{0,Z}$ classes $(\mathscr{W}_n : n \in \mathbb{N})$ is coded by a double-sequence of trees $(T_{n,i} : n, i \in \mathbb{N}) \leq_{\mathrm{T}} Z$.
- A **2-test** relative to Z is a uniform sequence of $\Sigma_2^{0,Z}$ classes $(\mathscr{W}_n : n \in \mathbb{N})$ such that $\forall n\left(\mu(\mathscr{W}_n) \leq 2^{-n}\right)$.

More formalized 2-randomness

A **2-test** relative to $Z \in 2^{\mathbb{N}}$ is a uniform sequence of $\Sigma_2^{0,Z}$ classes $(\mathscr{W}_n : n \in \mathbb{N})$ such that $\forall n \left(\mu(\mathscr{W}) \leq 2^{-n}\right)$.

$X \in 2^{\mathbb{N}}$ **passes** the 2-test $(\mathscr{W}_n : n \in \mathbb{N})$ if $X \notin \bigcap_{n \in \mathbb{N}} \mathscr{W}_n$.

X is **2-random** relative to Z if X passes every 2-test relative to Z.

Definition

2-MLR is the statement

$$\forall Z \, \exists X \, (X \text{ is 2-random relative to } Z).$$

Quick history

The definition of 2-randomness in terms of 2-tests is due to Kurtz.

The equivalence of 2-randomness (in terms of 2-tests) and ML-randomness relative to $0'$ is due to Kautz.

Among the first to consider 2-MLR in reverse mathematics are:

- Avigad, Dean, and Rute
- Conidis and Slaman

Mathematical consequences of 2-MLR

$\mathsf{RCA}_0 + 2\text{-}\mathsf{MLR}$ proves the **rainbow Ramsey theorem for pairs**. (Conidis and Slaman, following Csima and Mileti)

In fact, the rainbow Ramsey theorem for pairs is equivalent to 2-DNR over RCA_0. (J. Miller)

Rainbow Ramsey theorem for pairs:
Let $k \geq 1$, and let $f\colon [\mathbb{N}]^2 \to \mathbb{N}$ be ***k*-bounded**: $\forall n\,(|f^{-1}(n)| \leq k)$. Then there is an infinite $R \subseteq \mathbb{N}$ such that f is injective on $[R]^2$.

Over RCA_0, $2\text{-}\mathsf{MLR} + \mathsf{B}\Sigma^0_2$ is equivalent to a version of the dominated convergence theorem for Borel measures on compact Polish spaces. (Avigad, Dean, and Rute)

Dominated convergence theorem:
Let $\mathscr{X}$ be a compact Polish space, and let μ be a Borel measure on $\mathscr{X}$. Let $(f_n : n \in \mathbb{N})$, f, and g be members of $L^1(\mathscr{X})$ such that $(f_n : n \in \mathbb{N})$ converges to f pointwise and is dominated by g. Then $(\int f_n : n \in \mathbb{N})$ converges to $\int f$.

2-MLR versus W2R

$\mathsf{RCA}_0 + \text{2-MLR}$ is strictly between ACA_0 and $\mathsf{RCA}_0 + \mathsf{W2R}$ (and not above WKL_0).

Theorem (Nies and S.)

$\mathsf{RCA}_0 + \mathsf{W2R} \nvdash \text{2-MLR}$.

In fact, $\mathsf{RCA}_0 + \mathsf{W2R} \nvdash \text{2-DNR}$.

The immediate impulse is to use **van Lambalgen's theorem**: $X \oplus Y$ is random if and only if X is random and Y is random relative to X.

Therefore, if $X = \bigoplus_{n \in \mathbb{N}} X_n$ is random, then each X_i is random relative to $\bigoplus_{n<i} X_n$. So we can build a model of randomness from the columns of X.

However, van Lambalgen's theorem does **not** hold for weak 2-randomness.

So instead use van Lambalgen for ML-randomness, plus the fact that if $X \oplus Y$ has **hyperimmune-free degree** and Y is ML-random relative to X, then Y is also weakly 2-random relative to X.

Implications among randomness notions mentioned so far

Arrows indicate implications over RCA_0.

None of the arrows reverse. (Except the $\mathsf{CR} \Leftrightarrow \mathsf{SR}$ arrow, of course!)

$$
\begin{tikzcd}
 & \mathsf{ACA}_0 \arrow[ddl] \arrow[dr] & \\
 & & 2\text{-}\mathsf{MLR} \arrow[d] \\
\mathsf{WKL}_0 \arrow[dr] & & \mathsf{W2R} \arrow[dl] \\
 & \mathsf{MLR} \arrow[d] & \\
 & \mathsf{CR} \Leftrightarrow \mathsf{SR} \arrow[d] & \\
 & \mathsf{RCA}_0 &
\end{tikzcd}
$$

Quick slides on the first-order strength of 2-MLR

As far as I know, an **exact characterization** of the first-order consequences of $\mathsf{RCA}_0 + 2\text{-}\mathsf{MLR}$ is still an **open problem**.

Measure first-order strength via induction, bounding, and cardinality schemes:

$$\mathsf{B}\Sigma^0_2 \quad \Rightarrow \quad \mathsf{C}\Sigma^0_2 \quad \Rightarrow \quad \mathsf{I}\Sigma^0_1$$

- $\mathsf{I}\Sigma^0_1$ is the induction scheme for Σ^0_1 formulas.
- $\mathsf{C}\Sigma^0_2$ is a scheme saying that if $\varphi(x,y)$ is Σ^0_2 and defines an injection, then the range is unbounded.
- $\mathsf{B}\Sigma^0_2$ is the bounding scheme

$$(\forall n < a)(\exists m)\varphi(n,m) \rightarrow \exists b(\forall n < a)(\exists m < b)\varphi(n,m)$$

for Σ^0_2 formulas φ.

Quick slides on the first-order strength of 2-MLR

What is known:

- $\mathsf{RCA}_0 + 2\text{-}\mathsf{MLR} \vdash \mathsf{C}\Sigma^0_2$. (Conidis and Slaman)
- $\mathsf{RCA}_0 + \mathsf{B}\Sigma^0_2 + 2\text{-}\mathsf{MLR}$ is Π^1_1-conservative over $\mathsf{RCA}_0 + \mathsf{B}\Sigma^0_2$. (Conidis and Slaman)
- $\mathsf{RCA}_0 + 2\text{-}\mathsf{MLR} \nvdash \mathsf{B}\Sigma^0_2$. (Slaman)

So the first-order consequences of $\mathsf{RCA}_0 + 2\text{-}\mathsf{MLR}$ are strictly between those of RCA_0 and $\mathsf{RCA}_0 + \mathsf{B}\Sigma^0_2$.

Also, there are more recent results by Belanger, Chong, Wang, Wong, and Yang establishing a better upper bound on the first-order consequences of $\mathsf{RCA}_0 + 2\text{-}\mathsf{MLR}$.

Plain complexity and incompressibility

Let $C^Z(\sigma)$ denote the **plain Kolmogorov complexity** of a string $\sigma \in 2^{<\mathbb{N}}$ relative to a set $Z \in 2^{\mathbb{N}}$.

Slogan: $C^Z(\sigma)$ is the length of the shortest Z-description of σ.

- Fix a universal oracle Turing machine U (computing a partial function $2^{<\mathbb{N}} \to 2^{<\mathbb{N}}$ for each oracle).
- Define $C^Z(\sigma)$ to be $|\tau|$ for the shortest τ such that $U^Z(\tau) = \sigma$.

Definition

X is **infinitely often C^Z-incompressible** if

$$\exists b\ \exists^\infty m\ \left(C^Z(X{\restriction}m) \geq m - b\right).$$

Characterizing 2-randomness in terms of incompressibility

Recall: X is infinitely often C^Z-incompressible if $\exists b\, \exists^\infty m\, \left(C^Z(X\restriction m) \geq m - b\right)$.

Theorem (Nies, Stephan, and Terwijn; J. Miller indep. for $\Rightarrow$)

X is 2-random relative to Z $\quad\Leftrightarrow\quad$ X is infinitely often C^Z-incompressible.

Theorem (Nies and S.)

The equivalence between 2-randomness relative to Z and infinitely often C^Z-incompressibility is provable in RCA_0.

That is:

$$\mathsf{RCA}_0 \vdash \forall Z\, \forall X\, (X \text{ is 2-MLR relative to } Z \;\Leftrightarrow\; X \text{ is infinitely often } C^Z\text{-incomp.})$$

This is nice because infinitely often C^Z-incompressibility is easy to formalize in second-order arithmetic, but 2-randomness relative to Z is not.

Comments on the proof

Focus on the direction

X is 2-random relative to $Z \Rightarrow X$ is infinitely often C^Z-incompressible.

Main problem: Avoid using $\mathrm{B}\Sigma^0_2$!

Secondary consideration: Give a direct proof in terms of 2-tests.

$\mathrm{B}\Sigma^0_2$ tends to creep into arguments about computations relative to Z':

- Obtaining initial segments of Z' only requires bounded Σ^0_1 comprehension.
- Obtaining initial segments of an arbitrary $\Delta^{0,Z}_2$ set requires bounded Δ^0_2 comprehension, which is equivalent to $\mathrm{B}\Sigma^0_2$.

The original proofs think of 2-MLR as MLR-relative-to-Z':

- J. Miller's proof uses prefix-free complexity relative to Z'.
- Nies, Stephan, and Terwijn's proof uses the low basis theorem and MLR-relative-to-Z'.

Comments on the proof

We follow a proof by Bauwens, based on a proof by Bienvenu, Muchnik, Shen, and Vereshchagin.

The crux is the following lemma.

Lemma (Conidis)

Let $q \in \mathbb{Q}$ and let $(U_n : n \in \mathbb{N})$ be uniformly Z-r.e. sets such that $\forall n\, (\mu([\![U_n]\!]) \le q)$. Then for every $p > q$, there is a Z'-r.e. set V such that

$$\mu([\![V]\!]) \le p \qquad \textit{and} \qquad \forall n_0 \left(\bigcap_{i \ge n_0} [\![U_i]\!] \subseteq [\![V]\!] \right).$$

Supposing some X is **not** infinitely often C^Z-incompressible, the lemma is used to build a test capturing X.

Comments on the proof

We give a version of the lemma in RCA_0.

Lemma (RCA_0; Nies and S.)

Let $q \in \mathbb{Q}$ and let $(U_n : n \in \mathbb{N})$ be uniformly Z-r.e. sets such that $\forall n\, (\mu([\![U_n]\!]) \le q)$. Then for every $p > q$, there is a $\Sigma_2^{0,Z}$ class $\mathcal{V}$ such that

$$\mu([\![\mathcal{V}]\!]) \le p \qquad \textit{and} \qquad \forall n_0 \left(\bigcap_{i \ge n_0} [\![U_i]\!] \subseteq \mathcal{V} \right).$$

The basic idea is:

$$\text{replace} \qquad \bigcup_{n_0 \in \mathbb{N}} \bigcap_{i \ge n_0} [\![U_i]\!] \qquad \text{with} \qquad \mathcal{V} = \bigcup_{n_0 \in \mathbb{N}} \bigcap_{i = n_0}^{b_i} [\![U_i]\!]$$

for an appropriate sequence $b_0 < b_1 < b_2 < \cdots$.

Z' can compute the b_i's, but we want to **avoid** using Z'.

Balanced randomness and h-weak Demuth randomness

Let $h\colon \mathbb{N} \to \mathbb{N}$.

An **h-weak Demuth test** relative to Z is like an ML-test relative to Z, except you may change your mind about index of the n^{th} component U_n $h(n)$-many times.

X is **h-weakly Demuth random** relative to Z if X weakly passes every h-weak Demuth test relative to Z.

(In the context of Demuth randomness, the pros say 'weakly passes' instead of 'passes' to mean 'not in the intersection of the test.')

X is **balanced random** relative to Z if X weakly passes every $O(2^n)$-Demuth test relative to Z.

Definition

For h provably total in RCA_0, h-WDR is the statement

$$\forall Z\, \exists X\, (X \text{ is } h\text{-weakly Demuth random relative to } Z).$$

BR is the statement

$$\forall Z\, \exists X\, (X \text{ is balanced random relative to } Z).$$

MLR versus BR

MLR versus BR:

- Every balanced random set is Martin-Löf random.
- **Not** every Martin-Löf random set is balanced random.
- Yet if $X = X_0 \oplus X_1$ is ML-random, then either X_0 or X_1 is balanced random (Figueira, Hirschfeldt, Miller, Ng, Nies).

The original proof of the last item uses van Lambalgen's theorem and traceability notions (specifically, ω-r.e.-tracing).

We give a new direct proof that is easy to implement in RCA_0. Therefore:

Theorem (Nies and S.)

$\mathsf{RCA}_0 \vdash \mathsf{MLR} \Leftrightarrow \mathsf{BR}$.

MLR versus h-WDR and rates of growth

Recall:

- BR is (informally) $O(2^n)$-WDR.
- $\mathsf{RCA}_0 \vdash \mathsf{MLR} \Leftrightarrow \mathsf{BR}$.

If $h(n)$ grows faster than $n \mapsto k^n$ for every k, then h-WDR is stronger than MLR.

Theorem (Nies and S.)

Let $h\colon \mathbb{N} \to \mathbb{N}$ be such that:

- *h eventually dominates $n \mapsto k^n$ for every k*
- *$\mathsf{RCA}_0 \vdash h$ is total.*

Then $\mathsf{RCA}_0 + \mathsf{MLR} \nvdash h$-WDR. In fact, $\mathsf{WKL}_0 \nvdash h$-WDR.

To prove this:

- Build a model of WKL_0 in which $\forall X\, \exists k\, (X$ is k^n-r.e.$)$.
- If h eventually dominates k^n, then no k^n-r.e. set X is h-WDR.

Thank you!

Thank you for coming to my talk!
Do you have a question about it?