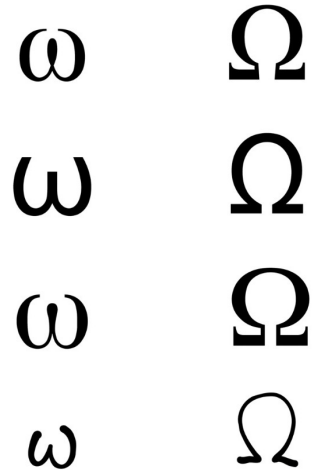
Martin-Löf randomness, 2-randomness, and reverse mathematics

André Nies, Uni Auckland

From ω to Ω, IMS, June 2023



Two questions motivated the present research

1. In work of Demuth in the 1980s, and then papers dating from 2009 onwards, several "almost everywhere" theorems from real analysis have been aligned with algorithmic randomness notions.

Can we align these theorems with axioms from reverse maths instead?

2. Many algorithmic randomness notions can be defined in the weak setting of RCA_0.

Can we prove the well known characterization and separation theorems about them in RCA_0?

The talk will give one sample answer to each question.

PART I: Lebesgue's theorem on a.e. differentiability in reverse maths

The reverse mathematics of theorems of Jordan and Lebesgue, JSL 2021, with Marcus Triplett and Keita Yokoyama

Lebesgue's theorem

We wish to determine the axiomatic strength over RCA_0 of the following classical result.

Theorem (Lebesgue, 1909)

Each nondecreasing function $f : [0,1] \to \mathbb{R}$ is differentiable almost everywhere.

- We will need an interpretation of "differentiable at x" that works within RCA_0.
- This will be "pseudo-differentiable" (Demuth), saying that the slopes around x converge as one zooms in.
- In this way we avoid asserting that the value of the derivative exists in the model (which is equivalent to ACA_0)

WWKL and MLR

- WWKL is "weak weak Königs lemma", saying that each binary tree of positive measure has an infinite path. It was introduced by Simpson and Yu, 1990.
- In the setting of RCA_0 a ML-test relative to X is given by an X-computable sequence of trees $\langle T_i \rangle_{i \in \mathbb{N}}$ such that $\mu(T_i) \geq 1 - 2^{-i}$, where $\mu(T_i)$ denotes $\lim_n 2^{-n} |T_i^{=n}|$.
- It describes the usual ML-test $\left\langle 2^{\mathbb{N}} - [T_i] \right\rangle_{i \in \mathbb{N}}$
- MLR is the axiom saying that for each X there is a ML-random relative to X
- Essentially by Kucera's work, $\mathsf{RCA}_0 \vdash \mathsf{MLR} \leftrightarrow \mathsf{WWKL}$.

A version of Lebesgue's theorem equivalent to WWKL

Theorem (N. Triplett Yokoyama, 2021 (2015, actually...))

The following are equivalent over RCA_0.

(A) WWKL

(B) every rationally presented nondecreasing function is pseudo-differentiable almost everywhere

- We refer to an encoding of functions via its values on the rationals, to be detailed shortly.
- We also need to say how to interpret "almost everywhere" in the limited setting of RCA_0.

Define pseudo-differentiability

Let $f :\subseteq [0,1] \to \mathbb{R}$ with domain containing $[0,1]_{\mathbb{Q}}$.

The slope of f at distinct reals a, b in its domain is

$$S_f(a,b) = \frac{f(b) - f(a)}{b - a}.$$

The h-derivative of f at $x \in [0,1]$, for a given $h > 0$, is the set of reals defined by

$$D_h f(x) = \{S_f(a,b) : a, b \in [0,1]_{\mathbb{Q}} \wedge a \leq x \leq b \wedge 0 < b - a < h\}.$$

f is pseudo-differentiable at $x \in (0,1)$ if

$$\lim_{h \to 0^+} \operatorname{diam}(D_h f(x)) = 0.$$

Define rationally presented

A function $g : [0,1]_{\mathbb{Q}} \to \mathbb{R} \setminus \mathbb{Q}$ has a set $Z \subseteq [0,1]_{\mathbb{Q}} \times \mathbb{Q}$ as a rational presentation if

- $g(p) < q \Rightarrow (p,q) \in Z$
- $g(p) > q \Rightarrow (p,q) \notin Z$.

Note that $g = g_Z$ where $g_Z(p) = \inf\{q \in \mathbb{Q} \colon\ (p,q) \in Z\}$.

Fact (RCA_0)

For each $f : [0,1]_{\mathbb{Q}} \to \mathbb{R}$ there is $\alpha \in \mathbb{R}$ such that $f + \alpha$ has a rational presentation.

Fact (RCA_0)

For each continuous function $h : [0,1] \to \mathbb{R}$ there is $\alpha \in \mathbb{R}$ such that $h + \alpha$ (restricted to $[0,1]_{\mathbb{Q}}$) has a rational presentation.

Explain "almost everywhere" in RCA_0 (1)

- A set $S \subseteq 2^{<\omega}$ is considered to be a code for the open set $[[S]]$.
- Let $T_S := \{\sigma \in 2^{<\omega} : \forall n < |\sigma| (\sigma \upharpoonright n \notin S)\}$.
- This forms a tree, which we view as a code of the complement of U.
- Define

$$\mu(S) := 1 - \mu(T) = 1 - \lim_{n \to \infty} \frac{|\{\sigma \in T : |\sigma = n\}|}{2^n}.$$

- While the (downward) limit may fail to exist in a model of RCA_0, one can still express that $\mu(S) \leq a$ or $\mu(T) \geq a$ by Π^0_1-formulas.

Explain "almost everywhere" in RCA_0 (2)

- We define the measure for an open set $U \subseteq 2^{\mathbb{N}}$ as
$$\widehat{\mu}(U) := \sup\{\mu(S) \mid U = [[S]]\}.$$
- Note $\widehat{\mu}(\emptyset) = 0$.
- $\pi : 2^{\mathbb{N}} \to [0,1]$ defined by $\pi(Z) = \sum_{n \in Z} 2^{-n}$.
- For an open set $U \subseteq [0,1]$ let $\widehat{\mu}(U) := \widehat{\mu}(\pi^{-1}(U))$.

Definition (Pseudo-differentiable a.e.)

Let $f :\subseteq [0,1] \to \mathbb{R}$ with domain containing $[0,1]_{\mathbb{Q}}$.
Say that f is pseudo-differentiable a.e. if:
$\widehat{\mu}(U) = 1$ for any open set $U \subseteq [0,1]$ that contains every point of pseudo-differentiability of f.

This implies pseudo-differentiable somewhere over RCA_0.

Theorem

The following are equivalent over RCA_0.

(A) WWKL

(B) every rationally presented, nondecreasing function is pseudo-differentiable a.e.

(B) $\to$(A)

Assume $\neg$(A). We first construct an open set $U \subseteq [0,1]$ such that $\widehat{\mu}(U) < 1$ and $[0,1] \setminus U$ only contains rationals. Next

- let $\{q_i\}_{i \in \mathbb{N}}$ be an enumeration of $[0,1]_{\mathbb{Q}}$
- define a function $f : [0,1]_{\mathbb{Q}} \to \mathbb{R}$ by $f(p) = \sum_{q_i < p} 2^{-i}$
- some vertical shift of f has a rational presentation
- f is nondecreasing and not pseudo-differentiable at any rational. So $\neg$(B).

Theorem (again)

The following are equivalent over RCA_0.

(A) WWKL

(B) every rationally presented nondecreasing function g is pseudo-differentiable a.e.

(A) $\to$(B)

- We adapt the proof of the result of Brattka/Miller/N. 2016: a nondecreasing computable function is differentiable at each computably random.
- They relied on the infinite pigeonhole principle $\mathsf{RT}^1_{<\infty}$ in one important place, which is equivalent to $B\Sigma_2$; we needed to circumvent that by changing the argument.

Functions of bounded variation

A function $f\colon [a,b] \to \mathbb{R}$ has bounded variation (BV) if the variation $V(f)$ is finite. Here

$$V(f) = \sup \sum_{i=0}^{n-1} |f(t_i + 1) - f(t_i)|$$

where the sup is taken over all partitions $a = t_0 \leq t_1 \leq \ldots \leq t_n = b$.

Let $f\colon [0,1] \to \mathbb{R}$ be a BV function. Jordan 1870s proved that $f = g_0 - g_1$ for some g_i that are nondecreasing. Here $g_0(x)$ is simply the variation of f restricted to $[0,x]$.

In the same paper (NTY 2021) we prove that over RCA_0, the version of Jordan's Theorem for continuous functions is $\leftrightarrow \mathsf{ACA}$ (also Kreutzer for "$\leftarrow$"), and the version for r.p. functions on $[0,1]_{\mathbb{Q}}$ is $\leftrightarrow \mathsf{WKL}$. This required modelling constructions of Greenberg, Miller, N. (IJM 2021) in RCA_0.

Theorem

The following are equivalent over RCA_0.

(A) WWKL

(C) every continuous BV function f is pseudo-differentiable a.e.

(D) every continuous BV function g is pseudo-differentiable somewhere.

(D) $\to$(A)

- If WWKL fails, then there is a tree $T \subseteq 2^{<\mathbb{N}}$ such that $[T] = \emptyset$ but $\mu(T) \geq \delta$ for some $\delta > 0$.
- Use this T as a base for a construction of a continuous BV function g that is a sum of finer and finer sawtooth functions.
- We can even make g absolutely continuous, and effectively uniformly continuous.

Theorem

The following are equivalent over RCA_0.

(A) WWKL

(C) every continuous BV function f is pseudo-diff'ble a.e.

$(A) \to (C)$

- Take a model (M, S) of WWKL_0. Can assume f is r.p.
- Take an open U such that $\widehat{\mu}(U) < 1$. We need to find $z \notin U$ such that f is pseudo-differentiable at z.
- There is a model $(M, \widehat{S})$ of WKL_0 such that $S \subseteq \widehat{S}$, and for each $A \in \widehat{S}$ there is $Z \in \mathcal{S}$ in MLR in A. (Simpson and Yokoyama).
- In $(M, \widehat{S})$ we have $f = g_0 - g_1$ for nondecreasing r.p. g_i. There is $Z \in S$ with Z MLR in $g_0 \oplus g_1 \oplus U$.
- We may assume $Z \notin U$ by taking tails a la Kucera.
- g_i are pseudo-diff'ble at real z corresponding to Z.

PART II:

2-randomness and incompressibility

Randomness notions and reverse mathematics,
JSL 2020, with Paul Shafer (who also contributed some presentation material)

Formalize 2-randomness in Z without using Z'

- A code for a $\Sigma^{0,Z}_2$ class $\mathcal{W}$ is a sequence of trees $(T_n : n \in \mathbb{N}) \leq_T Z$ such that $T_0 \subseteq T_1 \subseteq T_2 \subseteq \cdots$.
- Define $X \in \mathcal{W}$ if $\exists n \, (X \in [T_n])$.
- For $q \in \mathbb{Q}$, define $\mu(\mathcal{W}) \leq q$ if $\forall n \, ([T_n] \leq q)$.
- A uniform sequence of $\Sigma^{0,Z}_2$ classes $(\mathcal{W}_n)_{n\in\mathbb{N}}$ is coded by a double-sequence of trees $(T_{n,i})_{n,i\in\mathbb{N}} \leq_T Z$.
- A 2-test relative to Z is a uniform sequence of $\Sigma^{0,Z}_2$ classes $(\mathcal{W}_n)_{n\in\mathbb{N}}$ such that $\forall n \, (\mu(\mathcal{W}_n) \leq 2^{-n})$.
- X is 2-random relative to Z if $X \notin \bigcap_{n\in\mathbb{N}} \mathcal{W}_n$ for every 2-test relative to Z.

2-RAN is the statement "for each Z there is X that is 2-random relative to Z" (Avigad et al., 2012).

The strength of 2-RAN

2-RAN $+ B\Sigma_2$ is equivalent 2-WWKL, as well as a version of the dominated convergence theorem for Borel measures on compact Polish spaces (Avigad, Dean, and Rute, APAL 2012).

Let $C\Sigma_2$ say that the range of a Σ_2 injection is unbounded; this is between $B\Sigma_2$ and $I\Sigma_1$.

The first-order consequences of $\mathsf{RCA}_0 + $ 2-RAN are strictly between those of $\mathsf{RCA}_0 + B\Sigma_2$ and RCA_0:

- $\mathsf{RCA}_0 + $ 2-RAN $\vdash C\Sigma_2$ (Conidis and Slaman, JSL 2013).
- $\mathsf{RCA}_0 + $ 2-RAN $\nvdash B\Sigma_2$ (Slaman, unpubl.).
- There's now a better upper bound on the first-order consequences of $\mathsf{RCA}_0 + $ 2-RAN (Belanger, Chong, Wang, Wong, and Yang, TAMS 2021).

Plain complexity and incompressibility

Let $C(\sigma)$ denote the plain Kolmogorov complexity of a string $\sigma \in 2^{<\omega}$.

- Fix a universal oracle Turing machine $\mathbb{U}$ (computing a partial function $2^{<\omega} \to 2^{<\omega}$ for each oracle).
- Define $C(\sigma)$ to be $|\tau|$ for a shortest τ such that $\mathbb{U}(\tau) = \sigma$.
- RCA_0 can prove that this exists (because any nonempty Σ^0_1 set has a least element).

Definition

X is infinitely often C^Z-incompressible if

$$\exists b \ \exists^\infty m \ C^Z(X \upharpoonright m) \geq m - b.$$

Characterizing 2-randomness in terms of incompressibility

Theorem (N., Stephan, and Terwijn 2005; J. Miller 2004 independently for the harder implication $\Rightarrow$)

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

We will show that this is provable in RCA_0.

Problem: The original proofs think of 2-random in Z as ML-random in 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'.

Nonetheless...

Theorem (N. and Shafer, 2020)

$\mathsf{RCA}_0 \vdash \forall Z \ \forall X \ [X \text{ is 2-MLR relative to } Z \leftrightarrow X \text{ is infinitely often } C^Z\text{-incompressible}]$

- This is nice because it is straightforward to formalize the right hand side in second-order arithmetic via a Σ^0_4 formula.
- Study the first-order consequences of 2-RAN via its equivalent version in terms of i.o. incompressibility?

The proof of $\leftarrow$

Theorem (N. and Shafer, 2020)

$\mathsf{RCA}_0 \vdash \forall Z \ \forall X \ [X \text{ is 2-MLR relative to } Z \leftrightarrow X \text{ is infinitely often } C^Z\text{-incompressible}]$

- If X fails a 2-test relative Z, we need to show the i.o. compressibility.
- The original proof uses prefix free descriptive complexity K relative to $\emptyset'$. We need to avoid this.
- Instead, we follow an alternative proof given in Bienvenu et al., 2010.
- We formulate a parameterized version of the machine existence theorem for plain machines within RCA_0, and use it to get the compressing machine from the 2-test.

The proof of $\rightarrow$

Theorem (N. and Shafer, 2020)

$\mathsf{RCA}_0 \vdash \forall Z \ \forall X \ [X$ is 2-MLR relative to $Z \leftrightarrow$
X is infinitely often C^Z-incompressible$]$

Main problem: Avoid using $B\Sigma_2$. It is often applied in arguments about computations relative to Z'.
Secondary consideration: Give a direct proof in terms of 2-tests.

As usual prove the contraposition:

$$X \text{ a.e. } C^Z\text{-compressible} \rightarrow X \text{ not 2-random in } Z.$$

a.e. compressible $\to$ not 2-random, according to Bauwens

- Let $U_{b,i} = \{Y : C(Y \upharpoonright i) < i - b\}$ and note that $\mu(U_{b,i}) \leq 2^{-b}$ by counting descriptions.
- Suppose that for each b, the initial segment $X \upharpoonright i$ is eventually compressible by b. That is,
$$X \in \bigcup_{N \in \mathbb{N}} \bigcap_{i \geq N} U_{b,i}.$$
- Bauwens used a general covering lemma of Conidis (2012) which now provides a $\Sigma^0_1(\emptyset')$ class $\mathcal{V}_b$ such that $\mu(\mathcal{V}_b) \leq 2^{-b+1}$ and $\bigcup_{N \in \mathbb{N}} \bigcap_{i \geq N} U_{b,i} \subseteq \mathcal{V}_b$.
- By the uniformity of Conidis' lemma, we have a $\mathrm{ML}(\emptyset')$ test $(\mathcal{V}_{b+1})_{b \in \mathbb{N}}$ capturing X.

It suffices to prove a version of Conidis' lemma in RCA_0 where the covering sets are Σ^Z_2, i.e. encoded by sequences of trees as defined above.

Conidis' lemma in RCA_0

Lemma (RCA_0; N. and Shafer)

Let $b \in \mathbb{N}$ and let $(U_n : n \in \mathbb{N})$ be uniformly Z-r.e. sets such that $\forall n\ (\mu([[U_n]]) \leq 2^{-b})$. Uniformly in b and this sequence, there is a $\Sigma^{0,Z}_2$ class $\mathcal{V}$ such that

$$\mu(\mathcal{V}) \leq 2^{-b+1} \qquad \text{and} \qquad \forall N \bigcap_{i \geq N} [[U_i]] \subseteq \mathcal{V}.$$

The basic idea is:

$$\text{replace} \quad \bigcup_{N \in \mathbb{N}} \bigcap_{i \geq N} [[U_i]] \quad \text{with} \quad \mathcal{V} = \bigcup_{N \in \mathbb{N}} \bigcap_{i=N}^{b_N} [[U_i]]$$

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'.

Further alleyways to explore

1. Formulate and prove other equivalences from randomness theory in RCA_0. For instance, try (without asserting that Ω exists) to show

$$Z \text{ is 2-random} \Leftrightarrow Z \text{ is ML-random and low for } \Omega.$$

2. In RCA_0 show directly that

$\forall Z \exists X$ [X is infinitely often C^Z-incompressible] implies $C\Sigma_2$.

References

- *The reverse mathematics of theorems of Jordan and Lebesgue*, with Marcus Triplett and Keita Yokoyama, JSL 2021.

- *Randomness notions and reverse mathematics*, with Paul Shafer, JSL 2020.