Randomness connecting to set theory and to reverse mathematics

André Nies

June 2016

CIRM

Slides are on my web site under "talks".





Goals

- ► Connect randomness and computability to cardinal characteristics in set theory:
 - define a dual $\Delta(A)$ of the Gamma operator,
 - ► show $\Delta(A) > 0 \rightarrow \Delta(A) = 1/2$ by dualising Monin's proof
- ▶ Connect randomness to reverse mathematics:
 - study the axiom power needed to verify equivalence of randomness notions;
 - ▶ study strength of randomness existence axioms in the setting of reverse mathematics

PART I:

The Γ and Δ operators, and cardinal characteristics in set theory

The Γ operator

For $Z \subseteq \mathbb{N}$ the lower density is defined to be

$$\underline{\rho}(Z) = \liminf_{n} \frac{|Z \cap [0, n)|}{n}.$$

Recall that

$$\gamma(A) = \sup_{X \text{ computable}} \underline{\rho}(A \leftrightarrow X)$$

The Γ operator was introduced by Andrews, Cai, Diamondstone, Jockusch and Lempp (2013):

 $\Gamma(A) = \inf\{\gamma(Y) \colon Y \leq_T A\}.$

This only depends on the Turing degree of A.

Viewing $1 - \Gamma$ as a Hausdorff pseudodistance

For $Z \subseteq \mathbb{N}$ the upper density is defined by

$$\overline{\rho}(Z) = \limsup_{n} \frac{|Z \cap [0, n]|}{n}.$$

- ▶ For $X, Y \in 2^{\mathbb{N}}$ let $d(X, Y) = \overline{\rho}(X \triangle Y)$ be the upper density of the symmetric difference of X and Y
- ► this is a pseudodistance on Cantor space 2^N (that is, two objects may have distance 0 without being equal).

Let $\mathcal{R} \subseteq \mathcal{A} \subseteq M$ for a pseudometric space(M, d). The Hausdorff distance is $d_H(\mathcal{A}, \mathcal{R}) = \sup_{Y \in \mathcal{A}} \inf_{S \in \mathcal{R}} d(Y, S)$.

Given an oracle set A let $\mathcal{A} = \{Y \colon Y \leq_{\mathrm{T}} A\}$. Let $\mathcal{R} \subseteq \mathcal{A}$ denote the collection of computable sets. We have

 $1 - \Gamma(A) = d_H(\mathcal{A}, \mathcal{R}).$



Δ operator, a dual to Γ

 $\delta(Y) = \inf \{ \underline{\rho}(Y \leftrightarrow S) \colon S \text{ computable} \}$ $\Delta(A) = \sup \{ \delta(Y) \colon Y \leq_T A \}.$

- Γ(A) measures how well computable sets can approximate the sets that A computes.
 "Γ(A) > p" for fixed p ∈ [0, 1) is a lowness property.
- Δ(A) measures how well the sets that A computes can
 approximate the computable sets.

 "Δ(A) > p" is a highness property.

Interpreting $1 - \Delta(A)$ metrically

We can view $1 - \Delta(A)$ as a one-sided "dual" of the Hausdorff distance:

 $1 - \Delta(A) = d_H^*(\mathcal{A}, \mathcal{R}) = \inf_{Y \in \mathcal{A}} \sup_{S \in \mathcal{R}} d(Y, S).$



Example: for the unit disc $D \subseteq \mathbb{R}^2$ we have $d_H^*(D, D) = 1$.

 $\delta(Y) = \inf\{\underline{\rho}(Y \leftrightarrow S) \colon S \text{ computable}\}\$ $\Delta(A) = \sup\{\delta(Y) \colon Y \leq_T A\}.$

Properties of δ and Δ (w. Merkle and Stephan)

- ► $\delta(Y) \leq 1/2$ for each Y (by considering also the complement of S)
- ► Y Schnorr random $\Rightarrow \delta(Y) = 1/2$ (by law of large numbers)
- A computable $\Rightarrow \Delta(A) = 0.$
- ► $\Delta(A) = 0$ is possible for noncomputable A, e.g. if A is low and c.e., or 2-generic .

Cardinal characteristics and their analogs

We use analogs of cardinal characteristics in set theory. Consider a binary relation $R \subseteq \mathcal{X} \times \mathcal{Y}$ between sets, functions (or other objects encoded by reals).

▶ In set theory one lets

 $\mathfrak{b}(R) = \min\{|F| : F \subseteq \mathcal{X} \land \forall y \in \mathcal{Y} \exists x \in F [\neg x R y]\}$

(e.g. if R is almost everywhere domination of functions, one gets the unbounding number $\mathfrak{b})$

 $\mathcal{B}(R) = \{A \colon \exists y \leq_{\mathrm{T}} A \forall x \text{ computable } [xRy] \}$

(e.g., the same R yields highness.) See Rupprecht, Thesis, 2010; Brooke, Brendle, Ng, N., 2014.

The highness classes $\mathcal{B}(\sim_p)$

Definition (Brendle and N.) For $p \in [0, 1/2)$ let $S \sim_p Y$ if $\underline{\rho}(S \leftrightarrow Y) > p$, and $\mathcal{B}(\sim_p) = \{A: \exists Y \leq_{\mathrm{T}} A \forall S \text{ computable } S \sim_p Y\}.$

The connection to Δ : for each $p \in [0, 1/2)$ we have

$$\Delta(A) > p \Rightarrow A \in \mathcal{B}(\sim_p) \Rightarrow \Delta(A) \ge p.$$

We will show that all the classes $\mathcal{B}(\sim_p)$ coincide, for 0 . Therefore:

 $\Delta(A) > 0 \Rightarrow \Delta(A) = 1/2.$

A.e. avoiding a computable function

Definition $(\mathcal{B}(\neq^*, h))$

For a computable function h, we let $\mathcal{B}(\neq^*, h) = \{A: \exists f \leq_{\mathrm{T}} A, f < h \,\forall r \text{ computable} \\ \forall^{\infty} n f(n) \neq r(n) \}.$

▶ This gets easier as h grows faster.

▶ In the extreme, $\mathcal{B}(\neq^*)$, i.e. the class obtained when we omit the computable bound, coincides with "high or diagonally noncomputable".

Fact

A computes a Schnorr random $\Rightarrow A \in \mathcal{B}(\neq^*, 2^{\hat{h}})$ whenever \hat{h} is computable and $\infty > \sum_n 1/\hat{h}(n)$. E.g. $\hat{h}(n) = n^2$.

Recall: for $p \in (0, 1/2)$ let

 $\mathcal{B}(\sim_p) = \{A \colon \exists Y \leq_{\mathrm{T}} A \,\forall S \text{ computable } \underline{\rho}(S \leftrightarrow Y) > p\}.$

If A computes a Schnorr random then $A \in \mathcal{B}(\sim_p)$. $\mathcal{B}(\neq^*, h) = \{A: \exists f \leq_{\mathrm{T}} A, f < h \,\forall r \text{ computable} \\ \forall^{\infty} n \, r(n) \neq f(n) \}.$ If A computes a Schnorr random then $A \in \mathcal{B}(\neq^*, 2^{n^2})$.

Theorem (N., dual form of Monin's result) $\mathcal{B}(\sim_p) = \mathcal{B}(\neq^*, 2^{(2^n)})$ for each $p \in (0, 1/2)$.

Corollary

 $\Delta(A) > 0 \Leftrightarrow \Delta(A) = 1/2 \Leftrightarrow A \in \mathcal{B}(\neq^*, 2^{(2^n)}).$

Show the harder inclusion $\mathcal{B}(\sim_p) \supseteq \mathcal{B}(\neq^*, 2^{(2^n)})$: Relation 1: Let q > p such that q < 1/2. For $h(n) = 2^{\hat{h}(n)}$ and functions x, y < h, view x(n) as string of length $\hat{h}(n)$. $x \neq^*_{\hat{h},q} y \Leftrightarrow \forall^{\infty}n |\{i < \hat{h}(n) : x(n)(i) \neq y(n)(i)\}| \ge nq$. Relation 2: Let $L \in \mathbb{N}$ and u be a function. For a trace sconsisting of L-element sets, and a function y < u, let

 $s\not\ni_{u,L}^*y\Leftrightarrow\forall^{\infty}n[s(n)\not\ni y(n)].$

Four steps:

- 1. there is k such that where $\hat{h}(n) = \lfloor 2^{n/k} \rfloor$ $\mathcal{B}(\sim_p) \supseteq \mathcal{B}(\neq^*_{\hat{h},q}).$
- 2. There are $L \in \mathbb{N}$, $\epsilon > 0$ such that where $u(n) = 2^{\lfloor \epsilon \hat{h}(n) \rfloor}$, we have $\mathcal{B}(\neq_{\hat{h},q}^*) \supseteq \mathcal{B}(\not\ni_{u,L}^*)$.
- 3. $\mathcal{B}(\not\ni_{u,L}^*) \supseteq \mathcal{B}(\not\ni_{2^{(L2^n)},L}^*).$
- 4. Finally, $\mathcal{B}(\not\ni^*, 2^{(L2^n)}, L) \supseteq \mathcal{B}(\neq^*, 2^{(2^n)})$

Separations?

Recall: For a computable function h, we let $\mathcal{B}(\neq^*, h) = \{A: \exists f \leq_{\mathrm{T}} A, f < h \,\forall r \text{ computable} \\ \forall^{\infty} n \, f(n) \neq r(n) \}.$ It is easy to show $\mathcal{B}(\sim_0) \subset B(\neq^*, 2^{n!}).$

Question

Is $\mathcal{B}(1/4) \subset \mathcal{B}(\sim_0)$? Is $\mathcal{B}(\neq^*, 2^{(2^n)}) \subset \mathcal{B}(\neq^*, 2^{n!})$?

In fact we don't know much about any separations $\mathcal{B}(\neq^*, g) \subset \mathcal{B}(\neq^*, h)$ for $g \ll h$.

Maybe set theory can help: the analog of $\mathcal{B}(\neq^*,h)$ is the cardinal characteristic

 $\mathfrak{b}(\neq_h^*)$ = the least size of a set F of functions such that for each h-bounded function y,

there is a function $x \in F$ with $\exists^{\infty} n \ [x(n) = y(n)]$.

Separating the $\mathfrak{b}(\neq_h^*)$ in a suitable model of ZFC

 $\mathfrak{b}(\neq_h^*)$ = the least size of a set F of functions such that for each h-bounded function y, there is a function x in F with $\exists^{\infty} n \ [x(n) = y(n)].$

Theorem (Kamo and Osuga 2014, special case)

Let $\langle \lambda_n \rangle_{n < \omega}$ be a strictly increasing sequence of regular cardinals $> \aleph_0$, e.g. $\lambda_n = \aleph_{n+1}$.

There is a forcing notion $\mathbb P$ with the countable (anti)chain condition that forces:

there is a sequence of functions $\langle h_n \rangle_{n < \omega}$ in the ground model such that $\mathfrak{b}(\neq_{h_n}^*) = \lambda_n$ for each n.

The c.c.c. implies that cardinals remain cardinals.

PART II:

Randomness, analysis, reverse mathematics

Systems based on randomness notions

Let ${\sf C}$ denote a randomness notion. We study the strength of the subsystem of second-order arithmetic

 $\mathsf{C}_{\mathsf{0}} = \mathsf{RCA}_{\mathsf{0}} + \forall X \exists Y \, [Y \in \mathsf{C}^X].$

Notation:

- ▶ MLR is ML-randomness,
- ► CRand is computable randomness,
- **SRand** is Schnorr randomness.

 $\mathsf{MLR} \Rightarrow \mathsf{CRand} \Rightarrow \mathsf{SRand}$

We will also use C to denote the axiom $\forall X \exists Y [Y \in C^X]$.

Theorem (Simpson and X. Yu, 1990)

MLR is equivalent to WWKL over RCA_0 .

Formalising randomness notions

Care has to be taken how to formalise the corresponding systems. For instance we can't assume measure theory to define MLR, as this needs WWKL.

MLR

- ► 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 $\lim_n 2^{-n} |T_i^{=n}|$ (relative size of the *n*-th level). It simulates the ML-test $\langle 2^{\mathbb{N}} - [T_i] \rangle_{i \in \mathbb{N}}$
- ▶ Y is ML-random in X if for each such sequence, $Y \in [T_i]$ for some i.

CRand

Y is computably random in X if each martingale computable in X fails on Y.

Equivalences in the framework of reverse maths

Theorem (Yokoyama and N.)

Over RCA_0 , MLR is equivalent to the statements (suitably formulated)

- every continuous function of bounded variation is differentiable somewhere
- every continuous function of bounded variation is differentiable almost everywhere.

Original proof uses infinite pigeonhole principle $\mathsf{RT}^1_{<\infty}$ in one important place; we needed to get rid of that.

Equivalences in the framework of reverse maths

 $C^X(\sigma)$ denotes plain Kolmogorov complexity of σ relative to oracle X.

Theorem (Shafer and N.)

Over $B\Sigma_2$, 2Rand is equivalent to the statement for each X there is Z such that $\exists^{\infty} n C^X(Z \mid n) \ge n - O(1)$.

- ▶ Right-to-left actually works over RCA
- ▶ left-to-right may as well (wip).

Other equivalences left to be done: e.g. $2Rand \leftrightarrow MLR \cap Low(\Omega)$.

An ω -model of CRand_0 without a d.n.c. function

- ▶ Every high set is Turing above a computably random set (N., Stephan and Terwijn 2005).
- ▶ By the proof of Lemma 4.1 in Cholak, Greenberg, et al. 06, for each set *B* of non-d.n.c. degree there is a set *X*, high relative to *B*, such that $B \oplus X$ is also not of d.n.c. degree.
- Iterating this in the standard way, we build an ω -model of CRand_0 without a set of d.n.c. degree.
- ▶ In particular, there is no ML-random set.

$\mathsf{RCA}_0 \vdash \mathsf{SRand} \to \mathsf{CRand}$



Let \mathcal{M} be a model of SR_0 . Given a set X of \mathcal{M} , we want to find a set Y in \mathcal{M} that is computably random in X. Let Z be a set of \mathcal{M} that is Schnorr random in X.

- If Z is ML-random in X we are done.
- ▶ Else $Z \in \bigcap_m G_m$ for a ML-test $\langle G_m \rangle$ relative to X.
- ► Let $f(m) = \mu s. Z \in G_{m,s}$. Then $f \leq_{\mathrm{T}} Z \oplus X$, hence f exists in \mathcal{M} .
- ▶ There is no function $g \leq_{\mathrm{T}} X$ such that $f(k) \leq g(k)$ for infinitely many k (else $S_m = \bigcup_{k>m} G_{k,g(k)}$ defines a Schnorr test relative X that captures Z).
- ► Use f to build a martingale L that dominates all X-computable martingales. Let Y be a set on which L does not succeed.

$W2Rand_0 \not\vdash 2Rand$ shown by an ω -model

▶ Take a weakly 2-random Z that does not compute a 2-random.

For instance, a 2-random is not computably dominated. Any computably dominated ML-random Z is weakly 2-random and hence does not compute a 2-random.

For each n let Z_n be the n-th column of Z, that is, $Z_n = \{k: \langle k, n \rangle \in Z\}.$

- Let $\mathcal{M} = (\omega, \mathcal{S})$ where \mathcal{S} consists of all the sets Turing below the join of finitely many columns of Z.
- ▶ Z_n is weakly 2-random in any finite sum of columns not containing Z_n . So \mathcal{M} is a model of W2Rand₀.

Notions slightly stronger than MLR

An *h-Demuth test* for computable function *h* is an effective sequence $\langle \mathcal{U}_n \rangle$ of effectively open (Σ_1^0) subsets of Cantor space such that:

▶ For all *n*, the measure $\lambda(\mathcal{U}_n)$ of \mathcal{U}_n is bounded by 2^{-n}

► there is an *h*-c.e. function mapping *n* to a Σ_1^0 index for U_n .

A set Z is *h*-weakly Demuth random if $Z \notin \bigcap_n \mathcal{U}_n$ for every *h*-Demuth test. Z is balanced random if Z is $O(2^n)$ weakly Demuth random.

Proposition (Figueira et al. 2015)

Let $Z = Z_0 \oplus Z_1$ be ML-random. Then Z_0 or Z_1 is balanced random.

So MLR_0 + sufficient induction \vdash BalancedRd.

 $\mathsf{WKL}_0 \not\vdash 2^{n \log \log n} - \mathsf{weakDemRd} \text{ via } \omega\text{-model}$

Definition

For a computable function h, we say that a set Z is h-c.e. if there is a computable approximation such that $Z \upharpoonright n$ changes at most h(n) times.

Proposition (Shafer and N.)

There is an ω -model \mathcal{M} of WKL such that each set of \mathcal{M} is superlow and k^n -c.e. for some $k \in \mathbb{N}$.

- ▶ An *h*-c.e. set is not *h*-weak Demuth random.
- ▶ So \mathcal{M} satisfies WKL₀, but not the axiom for weak *h*-Demuth randomness, for any function *h* dominating all the functions k^n (e.g. $h(n) = 2^{n \log \log n}$).

References

J. Brendle, A. Brooke-Taylor, Keng Meng Ng, and A. Nies.

An analogy between cardinal characteristics and highness properties of oracles. In *Proceedings of the 13th Asian Logic Conference: Guangzhou, China*, pages 1–28. World Scientific, 2013. http://arxiv.org/abs/1404.2839.

- B. Monin and A. Nies. A unifying approach to the Gamma question. In *Proceedings of Logic in Computer Science* (*LICS*). IEEE press, 2015.
- A. Nies (editor). Logic Blog 2013.

Available at http://arxiv.org/abs/1403.5719, 2013.

A. Nies (editor). Logic Blog 2015.

Available at http://arxiv.org/abs/1602.04432, 2015.