Randomness Notions and Lowness Properties

André Nies

University of Auckland

www.cs.auckland.ac.nz/nies

February 2004

A source of examples

- Lots of recent research connects the areas of computability theory and randomness/Kolmogorov complexity
- Computability theory: a deep theory, but it does not have too many natural examples (the way say group theory has). For instance, a long open question by Sacks asks, in essence, if there is a natural r.e. set which is neither computable nor Turing -complete
- We will demonstrate how randomness/Kolmogorov complexity leads to new examples of natural classes and operators

Four classes

- Four classes of subsets of $\mathbb{N}$ have been introduced independently. They turn out to be the same!

Chaitin/Solovay	1975
Van Lambalgen/Zambella	1990
Kucera	1993
Muchnik jr	1999

- Each one captures some aspect of being far from random, or computationally weak
- First example of a natural Σ^0_3 ideal in the Turing degrees below the halting problem (i.e, the Δ^0_2 degrees).

$K(y)$

- A *machine* is a partial recursive function $M : \{0,1\}^* \mapsto \{0,1\}^*$.
- M is *prefix free* if its domain is an antichain under inclusion of strings.

Let $(M_d)_{d \geq 0}$ be an effective listing of all prefix free machines. The standard universal prefix free machine V is given by

$$V(0^d 1\sigma) = M_d(\sigma).$$

The prefix free version of Kolmogorov complexity is

$$K(y) = \min\{|\sigma| : V(\sigma) = y\}.$$

Thus, $K(y)$ is the length of a shortest prefix free description of y.

Class 1: anti-random

- For a string y, up to constants,

  $$K(|y|) \leq K(y)$$

  since we can compute $|y|$ from y (write numbers in binary).

- A set B is anti-random (also called K–trivial) if, for some $c \in \mathbb{N}$

  $$\forall n \; K(B \upharpoonright n) \leq K(n) + c,$$

  namely, the K complexity of all initial segments is minimal.

- each computable B is anti-random.

Why “anti-random”?

- An upper bound for $K(x)$ is $|x| + K(|x|) + \mathcal{O}(1)$, which is just a little above $|x|$ (as $K(n) \leq 2\log n$).
- Schnorr proved that a set Z is *Martin-Löf random* iff, for some c,

$$\forall n \; K(Z \upharpoonright n) \geq n - c$$

- So
  - Z is random if all complexities $K(Z \upharpoonright n$ are near the upper bound, while
  - Z is anti-random if they have the minimal possible value $K(n)$ (all within constants).

Why prefix free complexity?

If one would define anti-random using the usual Kolmogorov complexity C instead of K, then one obtained only the computable sets (Chaitin, 1975).

Solovay (1975) was the first to construct a non-computable anti-random A (which was Δ_2^0).

Constructions

After many intermediate results by various researchers, [Downey, Hirschfeldt, Nies, Stephan 2001] gave a two line "definition" of an r.e. non-computable anti-random set. We use the "cost function"

$$c(x, s) = \sum_{x<y\leq s} 2^{-K_s(y)}.$$

This determines a non-computable set A:

$A_s = A_{s-1} \cup \{x : \exists e$

- $W_{e,s} \cap A_{s-1} = \emptyset$ (haven't met e-th diagonalization requirement)
- $x \in W_{e,s}$ (can meet it, via x)
- $x \geq 2e$ (makes A co-infinite)
- $c(x, s) \leq 2^{-(e+2)}\}$. (Ensures A is anti-random.)

Post's problem

- Post, 1944 asked if there is an intermediate r.e. Turing degree.
- Friedberg and Muchnik (1955) independently gave affirmative answer, introducing priority method
- Kucera (1986) found a priority free solution
- Our construction has no priority/injury to requirements.
- We will see later that each anti-random A is low, $A' \leq_T \emptyset'$.
- So the construction gives a further priority free solution to Post's problem

Properties

Let $\mathcal{AR}$ be the class of anti-random sets.

Theorem 1 (Chaitin, 1975) $\mathcal{AR} \subseteq \Delta^0_2$.

Theorem 2 (DHNS, 2001) $\mathcal{AR}$ *is closed under* $\oplus$. *That is, if* $A, B \in \mathcal{AR}$, *then*

$$\{2x : x \in A\} \cup \{2x+1 : x \in B\} \in \mathcal{AR}.$$

Class 2: Kucera sets

The notion of ML-randomness relativizes, as does Schnorr's result. Thus, a set Z is MLRand^A if, for some c,

$$\forall n \; K^A(Z \upharpoonright n) \geq n - c.$$

Kucera (APAL, 1993) studied sets A such that

$$A \leq_T Z \text{ for some } Z \in \mathsf{MLRand}^A.$$

He called them "bases for 1-RRA".

We prefer "Kucera sets".

Restrictions:

- Each Kucera set is GL_1: $A' \leq_T A \oplus \emptyset'$.
- Downey, 2002: Each r.e. Kucera set is array recursive.

Kucera's construction

Theorem 3 (Kucera, 1993) *For each r.e. non-computable C, there is a non-computable r.e. Kucera set $A \leq_T C$. (And A is a Kucera set via a low Z.)*

The proof is an extension of K.'s method for priority free solution to Post's problem.

- Can assume C is low.
- By Low Basis Theorem relative to C, there is $Z \in \mathsf{MLRand}^C$, and Z low.
- Z is Δ^0_2 and "diagonally non-recursive", so one can build r.e. non-computable $A \leq_T Z$, which in addition satisfies $A \leq_T C$. Then Z is random in A.

Class 3: Low for random

- As an oracle A increases the power of tests, $\mathsf{MLRand}^A \subseteq \mathsf{MLRand}$.
- We say A is low for ML-random if $\mathsf{MLRand}^A = \mathsf{MLRand}$ (Zambella, 1990). $\mathsf{Low}(\mathsf{MLRand})$ denotes this class.
- Easy: each low for ML-random set is Kucera. For there is a ML-random Z such that $A \leq_T Z$. Then Z is ML-random relative to A.

Constructing one

Theorem 4 (Kucera and Terwijn, 1997) *There is a non-computable r.e. set in Low(ML-Rand).*

Their construction inspired ours on anti-random.

Kucera/Terwijn asked if there is a low for random set not in Δ^0_2. (This is also Problem 4.4. in Ambos-Spies/ Kucera, 2000).

$\mathrm{Low}(\mathsf{MLRand}) \subseteq \mathcal{AR}$

Theorem 5 (Nies 2001) *If A is low for random, then A is anti-random.*

- In particular, $A \leq_T \emptyset'$ by Chaitin's result. This answers the question of Kucera and Terwijn in the negative.
- Since Kucera sets are GL_1, in fact $A' \leq_T \emptyset'$
- Proof: complicated. Uses martingales.

Kucera ⇒ anti-random

Hirschfeldt and Nies worked in Rio de Janeiro, December 2003, and proved:

Theorem 6 *If A is Kucera, then A is anti-random.*

- This improves the previous Theorem, and the proof is simpler!
- However, the more complex earlier proof extends to other randomness notions (as we will see later).
- Interestingly, Turing reducibility helps to clarify the relationship between two notions, low for random and anti-random, which are not directly related to it.

The proof idea

- Suppose $A = \Phi(Z)$ for some $Z \in \mathsf{MLRand}^A$, where Φ is a Turing reduction.

- We want to enumerate a prefix-free machine M such that for some d, for each n, there is a description $M(\sigma) = A \upharpoonright n$, $|\sigma| \leq K(n) + d$. We don't know what A is and only have a limited amount of descriptions.

- There must be many oracle strings τ, such that $A \upharpoonright n \preceq \Phi^\tau$, else Z is not A-random.

- When we see enough τ's, we can issue the description.

- d is a number such that $Z \notin V_d$, where (V_d) is an appropriate ML-test relative to A.

Inclusions, so far:

$$\mathrm{Low}(\mathsf{MLRand}) \subseteq \mathrm{Kucera} \subseteq \mathcal{AR}$$

The blue inclusions $\subseteq$ are non-trivial.

(Also: $\mathcal{AR} \subseteq \Delta^0_2$)

What about equality?

What is the 4th class?

Class 4: low for K

In general, adding an oracle A decreases $K(y)$.

A is low for K if this is not so. In other words,

$$\forall y\ K(y) \leq K^A(y) + \mathcal{O}(1).$$

Let $\mathcal{M}$ denote this class. It was introduced by Andrej Muchnik (1999), who proved there is an r.e. noncomputable $A \in \mathcal{M}$.

Trivially, $\mathcal{M} \subseteq \mathsf{Low}(\mathsf{MLRand})$, as

- MLRand can be defined in terms of K, and
- MLRand^A in terms of K^A.

Inclusions, so far:

$$\mathcal{M} \subseteq \mathrm{Low}(\mathsf{MLRand}) \subseteq \mathrm{Kucera} \subseteq \mathcal{AR}$$

Downward closure

Theorem 7 *If $A \in \mathcal{AR}$ and $B \leq_T A$, then $B \in \mathcal{AR}$.*

- This is hard, since a reduction $B \leq_T A$ generally uses a lot of the oracle A to compute $B \restriction n$.

- The proof started from the [DHNS 2001] result that no anti-random is Turing complete.

- The construction uses a model similar to pinball machines, but the balls are replaced by arbitrarily small quantities of liquid. I call it the "decanter model" (see upcoming bulletin paper by DHNT).

- B is anti-random because it can be viewed as being constructed via the cost-function method. As a corollary (where $B = A$), this method characterizes the anti-random sets.

All is one

The remaining inclusion $\mathcal{AR} \subseteq \mathcal{M}$ follows by slightly modifying the construction for the previous theorem.

Theorem 8 (with Hirschfeldt) *Each anti-random set is low for K.*

Non-uniformity

The proofs of the previous two theorems are rather complex. However, there seems to be a reason: $\mathcal{AR} \subseteq \mathcal{M}$ is non-effective.

Theorem 9 (with Hirschfeldt) *There is no effective way to do this:*

- *given an r.e. index for A and a constant b such that A is anti-random via b*
- *obtain a constant d such that A is low for K via d.*

This is because one can effectively list $\mathcal{AR}$ with constants for being anti-random, but not with constants for being low for K.

Further results

The sets in $\mathcal{AR}$ form an ideal in the Δ_2^0 Turing degrees, such that

- the ideal $\mathcal{AR}$ is generated by its r.e. members
- $\mathcal{AR}$ is Σ_3^0
- $\mathcal{AR}$, like any Σ_3^0 ideal, is contained in $\subseteq [\mathbf{o}, \boldsymbol{b}]$ for some r.e. Low_2 $\boldsymbol{b}$
- each $A \in \mathcal{AR}$ is low.

Also, $X \equiv_T Y$ implies $\mathcal{AR}^X = \mathcal{AR}^Y$.

Why does this class come up in so many different ways? I don't know.

Chaitin's Ω

Chaitin defined the halting probability Ω_U, for a universal prefix-free machine U, to be

$$\Omega_U = \sum\{2^{-|\sigma|} : \ U(\sigma)\downarrow\}$$

- The left cut given by Ω_U is r.e. (we say Ω_U is left-r.e.)
- Ω_U is random (rather, its binary expansion)
- Each left-r.e. random real number is some Ω_U (Calude e.a. 1999; Kucera and Slaman 2001)
- $\Omega_U \equiv_T \emptyset'$.

Relativizing Ω

For an oracle X,

$$\Omega_U^X = \sum\{2^{-|\sigma|} : U^X(\sigma)\downarrow\}$$

- Ω_U^X is random relative to X. In particular, $\Omega_U^X \not\leq_T X$
- If $A \leq_T \Omega_U^A$, then A is a Kucera set and hence anti-random. So for “about every” set, A and Ω_U^A are Turing incomparable.

When is Ω_U^A left-r.e.?

For Δ_2^0 sets A, Ω_U^A left-r.e. implies $A \leq_T \Omega_U^A$, hence A is anti-random. Converse:

Theorem 10 (Nies, Dec 2003) *If A is anti-random, then Ω_U^A is left-r.e.*

A persistent open question is whether for some U (say,the standard one), $X \equiv_T Y$ implies $\Omega_U^X \equiv_T \Omega_U^Y$. By the last result, this is true at least for anti-random sets X.

Downey has announced that there is a properly Σ_2^0 set A such that Ω_U^A is left-r.e.

Martingales

A martingale is a function $M : \{0,1\}^* \mapsto \mathbb{R}_0^+$ such that

$$M(x0) + M(x1) = 2M(x)$$

Intuition:

- When we have seen the initial segment x, we bet an amount $\beta, 0 \le \beta \le M(x)$ that the next bit has a certain value, say 0.
- If next bit **is** 0, we win β, else we loose β.

M succeeds on Z if

$$\limsup_n M(Z \restriction n) = \infty.$$

CRand and NMRand

- Z is computably random (CRand) if **no** computable martingale M succeeds on Z. That is, $M(Z \upharpoonright n)$ is bounded.
- While a martingale always bets on the **next** position, a non-monotonic betting strategy can choose some position that has not been visited yet.
- Z is non-monotonic random (NMRand) if no non-monotonic betting strategy succeeds on Z.

$$\mathsf{MLRand} \subseteq \mathsf{NMRand} \subset \mathsf{CRand}.$$

But it is a major open problem if the first inclusion is proper, too.

Lowness notions

The following is a further improvement of the original result (Nies 2002) that $\mathsf{Low}(\mathsf{MLRand}) \subseteq \mathcal{AR}$.

Theorem 11 *If* $\mathsf{MLRand} \subseteq \mathrm{CRand}^A$ *then* A *is anti-random.*

(The converse implication holds, too, since $\mathcal{AR} \subseteq \mathcal{M}$.)

If A is low for NMRand, then

$$\mathsf{MLRand} \subseteq \mathsf{NMRand} = \mathsf{NMRand}^A \subseteq \mathsf{CRand}^A.$$

Thus

Corollary 12 *Each low for NMRand set is anti-random.*

Low(CRand)

Earlier result:

Theorem 13 (with B. Bedregal, Natal)
Each Low(CRand) set is hyper-immune free.

But also, by Theorem 11 each Low(CRand) set is anti-random, hence Δ^0_2. Since the only hyper-immune free Δ^0_2 are the computable sets, this implies, as conjectured by Downey,

Theorem 14 *If A is Low(CRand) then A is computable.*

This answers **Question 4.8** in Ambos-Spies/Kucera (1999) in the negative.