

# Relative Randomness:

## Interactions between Initial Segment Kolmogorov Complexity of Sets and Computability Theory

### A Very Partial Progress Report

Denis R. Hirschfeldt  
University of Chicago

---

Slides for a talk presented at the Seminar on Kolmogorov Complexity and Applications, Schloss Dagstuhl, Germany, Jan. – Feb. 2006.

A road trip with detours through some of the landscape of recent results on relative effective randomness. Much has been left out, but I hope these give an idea of some of the current concerns in this area of research.

References:

*Calibrating Randomness*

Downey, Hirschfeldt, Nies, and Terwijn

<http://www.uchicago.edu/~drh>.

*Randomness and Computability: Open Questions*

Miller and Nies

<http://www.cs.auckland.ac.nz/~nies>.

*Some Recent Progress in Algorithmic Randomness*

Downey

<http://www.mcs.vuw.ac.nz/research/maths-pubs.shtml>.

*Algorithmic Randomness and Complexity*

Downey and Hirschfeldt

<http://www.mcs.vuw.ac.nz/~downey>  
(very rough draft).

## Basic Concepts:

- $C$ : plain Kolmogorov complexity
- $K$ : prefix-free Kolmogorov complexity
- All sets are subsets of  $\mathbb{N}$ , which we can think of as infinite binary strings or as reals in  $[0, 1]$ .
- $\leq_{\text{T}}$ : Turing reducibility
- $\leq_{\text{wtt}}$ : weak truth table reducibility
- $\leq_{\text{tt}}$ : truth table reducibility
- $X'$ : the Halting Problem relative to  $X$
- $X^{(n)}$ : the Halting Problem relative to  $X^{(n-1)}$
- $A \oplus B = \{2n \mid n \in A\} \cup \{2n + 1 \mid n \in B\}$ .

- A set  $A$  is 1-random if

$$K(A \upharpoonright n) \geq n - O(1).$$

- [**Schnorr**] This definition is equivalent to Martin-Löf's original definition.
- Example:  $\Omega = \sum_{\sigma \in \text{dom } U} 2^{-|\sigma|}$ , where  $U$  is a universal prefix-free machine. [**Chaitin**]
- [**Martin-Löf**] There is no  $X$  such that

$$C(X \upharpoonright n) \geq n - O(1).$$

- [**Miller and Yu**] A set  $A$  is 1-random iff for every computable  $g$  s.t.  $\sum_n 2^{-g(n)} < \infty$ ,

$$C(A \upharpoonright n) \geq n - g(n) - O(1).$$

• If  $A$  is 1-random then:

1. [Chaitin]  $\lim_n K(A \upharpoonright n) - n = \infty$ .

2. [Solovay] For any computable  $f$  s.t.  
 $\sum_n 2^{-f(n)} = \infty$ ,

$$\exists^\infty n [K(A \upharpoonright n) > n + f(n)].$$

• [Miller and Yu] TFAE

1.  $A$  is 1-random.

2.  $\sum_n 2^{n-K(A \upharpoonright n)} < \infty$ .

3. For any  $f$  s.t.  $\sum_n 2^{-f(n)} = \infty$ ,

$$\exists^\infty n [K(A \upharpoonright n) > n + f(n)].$$

4.  $C(A \upharpoonright n) \geq n - K(n) - O(1)$ .

- [Gács; Kučera] Every set is wtt-reducible to a 1-random set.
- The bound on this wtt-reduction:
  - can be  $n + o(n)$  [see Merkle and Mihailović];
  - cannot be  $n + O(1)$  [Hirschfeldt].
- **Open Questions:** Given  $A$ , is there always a 1-random  $R$  s.t.  $A \leq_K R$ , that is,

$$K(A \upharpoonright n) \leq K(R \upharpoonright n) + O(1)?$$

What about one s.t.  $A \leq_{rK} R$ , that is,

$$K(A \upharpoonright n \mid R \upharpoonright n) \leq O(1)?$$

- This thm is a bit distressing, because random sets shouldn't be computationally powerful.
- Miller's Heuristic: The more random a set, the less useful it is.

- A set  $A$  is 1-random relative to  $X$  if

$$K^X(A \upharpoonright n) \geq n - O(1).$$

- A set  $A$  is  $n$ -random if it is 1-random relative to  $\emptyset^{(n-1)}$ .

- So for instance,  $A$  is 2-random if

$$K^{\emptyset'}(A \upharpoonright n) \geq n - O(1).$$

- There are 1-random sets  $\leq_T \emptyset'$ , but no 2-random sets.

- It is sometimes possible to give unrelativized characterizations of these relativized notions.

- **[Nies, Stephan, and Terwijn; Miller for one direction]** A set  $A$  is 2-random iff

$$\exists^\infty n (C(A \upharpoonright n) \geq n - O(1)).$$

- It then follows from work of Solovay that if

$$\exists^\infty n (K(A \upharpoonright n) \geq n + K(n) - O(1)). \quad (1)$$

then  $A$  is 2-random.

- **[Yu, Ding, and Downey; implicit in Solovay]** If  $A$  is 3-random then (1) holds.

- **Open Question:** Is (1) equivalent to 2-randomness, 3-randomness, or neither?

Examples of Miller's Heuristic in Action:

- [**Sacks and Stillwell; see Kautz**] If  $A$  is 2-random then  $A$  is  $GL_1$ :

$$A' \equiv_T A \oplus \emptyset'.$$

- [**Nies, Stephan, and Terwijn**] A 1-random set  $A$  is 2-random iff  $\Omega$  is 1-random relative to  $A$ .

- [**Miller**] If  $A$  is 3-random then

$$\exists^\infty n (K(n) \leq K^A(n) + O(1)).$$

- [**Miller**] If  $A$  is 3-random and  $A \leq_K B$  then  $B \leq_T A \oplus \emptyset'$  and  $B' \leq_T A'$ .

- [**Miller and Yu**] If  $A$  is  $n$ -random and  $B \leq_T A$  is 1-random, then  $B$  is  $n$ -random.

- So it seems that Miller's Heuristic begins to work at the 2-random level.
- However, we can see it working even at the 1-random level once we get rid of some "fake" 1-random sets.
- In the proofs of the Kučera-Gács Theorem, the random reals constructed always compute  $\emptyset'$ .
- A set  $A$  is *PA-complete* if every infinite computable binary tree has an  $A$ -computable path.
- **[Stephan]** If  $A \not\leq_T \emptyset'$  is 1-random then  $A$  is not PA-complete.
- We will later see another qualitative difference between the 1-random sets above  $\emptyset'$  and other 1-random sets.

- Note that among the “fake” 1-random sets is  $\Omega$ .
- $\Omega$  is a *left-c.e. real*, that is, there is a computable sequence of rationals

$$q_0 < q_1 < \dots \rightarrow \Omega.$$

- So  $\Omega$  has c.e. Turing degree.
- [**Kučera**] If a 1-random set  $A$  has c.e. Turing degree then  $A \equiv_T \emptyset'$ .
- [**Calude and Nies**] If  $A$  is a 1-random left-c.e. real then  $A \equiv_{\text{wtt}} \emptyset'$ .
- [**Demuth**] If  $A$  is 1-random and  $B \leq_{\text{tt}} A$  is noncomputable then there is 1-random  $C \equiv_T B$ .
- So no 1-random set is  $\geq_{\text{tt}} \emptyset'$ .

- Kučera and Slaman gave a characterization of the 1-random left-c.e. reals in terms of a strong reducibility called Solovay reducibility,  $\leq_s$ .
- In particular, if  $A$  and  $B$  are 1-random left-c.e. reals then  $A \equiv_K B$ .
- There is a theory of “measures of relative randomness” that works particularly well on the left-c.e. reals.
- For example, for left-c.e. reals  $A$  and  $B$ , their sum  $A + B$  is a natural join with respect to such measures.

- To be precise, let us choose one such measure, say  $A \leq_{\text{rK}} B$ :

$$K(A \upharpoonright n \mid B \upharpoonright n) \leq O(1).$$

- This works exactly the same for  $\leq_K$ ,  $\leq_S$ , etc.
- It follows from the Kučera-Slaman Theorem that all 1-random left-c.e. reals are rK-equivalent.
- Let  $A, B, C$  in this and the next slide be left-c.e. reals.
- Then  $A, B \leq_{\text{rK}} A + B$ ,
- and if  $A, B \leq_{\text{rK}} C$  then  $A + B \leq_{\text{rK}} C$ .
- It's natural for computability theorists to ask about structural properties of degree structures arising from reducibilities measuring relative randomness.

- [Downey, Hirschfeldt, LaForte, Nies] The S-degrees, rK-degrees, K-degrees, etc. of left-c.e. reals are dense. E.g., if  $A <_{rK} B$  then there is a  $C$  such that  $A <_{rK} C <_{rK} B$ .

- [Downey, Hirschfeldt, and LaForte] If  $C$  is not 1-random then there are  $A, B <_{rK} C$  such that  $A + B \equiv_{rK} C$ .

- [Demuth; see Downey, Hirschfeldt, and Nies] If  $C = A + B$  is 1-random then at least one of  $A$  and  $B$  is 1-random (and hence rK-equivalent to  $C$ ).

- Another reason to further investigate the Kučera-Gács Theorem is the following classical result.

- [de Leeuw, Moore, Shannon and Shapiro; Sacks] If  $A$  is not computable then

$$\mu(\{X : X \geq_T A\}) = 0.$$

- The Kučera-Gács Theorem gives a sense in which this theorem cannot be effectivized.

- A set  $A$  is a *basis for 1-randomness* if there is an  $R \geq_T A$  that is 1-random relative to  $A$ .

- [Kučera] Every basis for 1-randomness is  $GL_1$ .

- In particular,  $\emptyset'$  is not a basis for 1-randomness, so there is no 2-random set  $\geq_T \emptyset'$ .

- Being a basis for 1-randomness is a notion of randomness-related computational weakness.
  - There are other such notions:
  - A set  $A$  is *low for 1-randomness* if every 1-random set is 1-random relative to  $A$ .
  - A set  $A$  is *low for  $K$*  if  $K(n) \leq K^A(n) + O(1)$ .
  - Noncomputable examples of such sets do exist, and can be computably enumerable.
- [Kučera / Kučera and Terwijn / Muchnik]**
- low for  $K \Rightarrow$  low for 1-randomness  $\Rightarrow$  basis for 1-randomness
  - We can characterize these classes of sets exactly using Kolmogorov complexity.

- A set  $A$  is *K-trivial* if  $K(A \upharpoonright n) \leq K(n) + O(1)$ .
- Note that  $A$  is K-trivial iff  $A \leq_K \emptyset$ .
- Computable sets are *K-trivial*, but there are also noncomputable ones. [**Solovay**]
- The corresponding notion of *C-triviality* holds of only the computable sets. [**Chaitin**]
- [**Chaitin**] If  $A$  is *K-trivial* then  $A \leq_T \emptyset'$ .
- [**Downey, Hirschfeldt, Nies, and Stephan**]  
If  $A$  is *K-trivial* then  $A <_T \emptyset'$ .

- [Nies] If  $A$  is  $K$ -trivial then  $A$  is low:  $A' \equiv_{\text{T}} \emptyset'$ .
- [Nies] If  $A$  is  $K$ -trivial and  $B \leq_{\text{T}} A$  then  $B$  is  $K$ -trivial.
- [Downey, Hirschfeldt, Nies, and Stephan]  
If  $A$  and  $B$  are  $K$ -trivial then so is  $A \oplus B$ .
- So the  $K$ -trivial sets form an ideal.

- **[Nies]** A set is  $K$ -trivial iff it is low for 1-randomness.
- **[Hirschfeldt and Nies]** If a set is  $K$ -trivial then it is low for  $K$ .
- **[Hirschfeldt, Nies, and Stephan]** If a set is a basis for 1-randomness then it is  $K$ -trivial.
- We already saw that low for  $K \Rightarrow$  basis for 1-randomness, so:
  - TFAE
    1.  $A$  is  $K$ -trivial.
    2.  $A$  is low for 1-randomness.
    3.  $A$  is low for  $K$ .
    4.  $A$  is a basis for 1-randomness.

An application:

- $\mathcal{A} \subset 2^{\mathbb{N}}$  is a *Scott Set* if
  1.  $(X \in \mathcal{A} \wedge Y \leq_T X) \Rightarrow Y \in \mathcal{A}$ ;
  2.  $X, Y \in \mathcal{A} \Rightarrow X \oplus Y \in \mathcal{A}$ ; and
  3. if  $T \in \mathcal{A}$  codes an infinite binary branching tree, then there is a  $P \in \mathcal{A}$  coding a path in this tree.

**Question [Friedman; McAllister]:** If  $\mathcal{A}$  is a Scott Set and  $X \in \mathcal{A}$  is not computable, must there be a  $Y \in \mathcal{A}$  s.t.  $X \mid_T Y$ ?

- [Kučera] The answer is yes if  $X$  is not a basis for 1-randomness.
- [Slaman] The answer is also yes if  $X$  is  $K$ -trivial, and hence the answer to the full question is yes.

- Back to structural properties of measures of relative randomness:

- $\leq_S, \leq_{rK}$ , etc. imply  $\leq_T$ , so their degree structures contain minimal pairs. E.g., there are  $A, B$  s.t. if  $C \leq_{rK} A, B$  then  $C \leq_{rK} \emptyset$  (i.e.,  $C$  is computable).

- What about  $\leq_K$ ?

- [**Csima and Montalbán**] There is a minimal pair of  $K$ -degrees, that is,  $A, B$ , s.t. if  $C \leq_K A, B$  then  $C \leq_K \emptyset$  (i.e.,  $C$  is  $K$ -trivial).

- [**Csima and Montalbán**] There is a nondecreasing unbounded  $f$  s.t. if  $A$  is not  $K$ -trivial then

$$K(A \upharpoonright n) \geq K(n) + f(n) - O(1).$$

• [Miller and Yu] Let  $\Omega_n = \{x \mid \langle x, n \rangle \in \Omega\}$ .  
Then  $\Omega_m \not\leq_K \Omega_n$  for  $m \neq n$ .

• But are there comparable K-degrees of  
1-random sets?

• Recall:  $A$  is 1-random iff For any  $f$  s.t.  
 $\sum_n 2^{-f(n)} = \infty$ ,

$$\exists^\infty n [K(A \upharpoonright n) > n + f(n)].$$

[Miller and Yu]

• [Miller and Yu] Let  $f$  be s.t.  $\sum_n 2^{-f(n)} < \infty$ .  
There is a 1-random  $A$  s.t.

$$K(A \upharpoonright n) \leq n + f(n) + O(1).$$

So for a 1-random  $A$ , there's a 1-random  $B <_K A$ .

- Returning to the distinction between 1-random sets above  $\emptyset'$  and other 1-random sets, we have:

- [**Hirschfeldt, Nies, and Stephan**] If  $R \not\leq_T \emptyset'$  is 1-random and  $A \leq_T R$  is c.e. then  $A$  is  $K$ -trivial.

- **Open Question:** Is every  $K$ -trivial set computable in a 1-random set  $\not\leq_T \emptyset'$ ?

- Here computable enumerability doesn't matter, because every  $K$ -trivial set is computable in a c.e.  $K$ -trivial set. [**Nies**]

- [**Kautz**] If  $A$  and  $B$  are 2-random relative to each other then every set  $\leq_T A, B$  is computable.

- [**Kučera**] If  $A, B \leq_T \emptyset'$  are 1-random then there is a noncomputable set  $\leq_T A, B$ .

- [**Hirschfeldt, Nies, and Stephan**] If  $A$  and  $B$  are 1-random relative to each other then every set  $\leq_T A, B$  is  $K$ -trivial.

- We can relativize  $\Omega$  to a given set  $A$ , by letting

$$\Omega^A = \sum_{\sigma \in \text{dom } U^A} 2^{-|\sigma|},$$

where  $U$  is a universal prefix-free oracle machine.

- Then  $\Omega^A$  is 1-random relative to  $A$ , and  $\Omega^A \oplus A \equiv_T A'$ .
- If  $A \leq_T \emptyset'$  is not  $K$ -trivial, then  $\Omega^A \not\equiv_T A$ , so  $\Omega^A \not\equiv_T \emptyset'$ .
- So if  $A \leq_T \emptyset'$  is not  $K$ -trivial, then there is a 1-random  $R \not\equiv_T \emptyset'$  s.t.  $R \oplus A \geq_T \emptyset'$ .

- [Nies] There is a c.e. set  $B$  such that if  $R$  is 1-random and  $R \oplus B \geq_{\text{T}} \emptyset'$ , then  $R \geq_{\text{T}} \emptyset'$ .

- **Open Question:** Does every  $K$ -trivial set  $B$  have this property?

- [Hirschfeldt and Nies] If  $B$  is  $K$ -trivial,  $R$  is 1-random, and  $R \oplus B \geq_{\text{T}} \emptyset'$ , then  $\emptyset'$  is  $K$ -trivial relative to  $R$ , that is,

$$K^R(\emptyset' \upharpoonright n) \leq K^R(n) + O(1).$$

- There's much space for different initial segment complexities between  $K$ -trivial and 1-random.
- A set  $A$  has  $\Sigma_1^0$ -dimension  $r$  if

$$\liminf_n \frac{K(A \upharpoonright n)}{n} = r.$$

- This form of the definition is due to Mayordomo.
- **Open Questions:** If  $A$  has  $\Sigma_1^0$ -dimension  $r > 0$ , must there be a  $B \leq_T A$  with  $\Sigma_1^0$ -dimension  $> r$ ?

If  $A$  has  $\Sigma_1^0$ -dimension  $> 0$ , must there be a 1-random  $B \leq_T A$ ?

What if  $A$  has  $\Sigma_1^0$ -dimension 1?

- **[Nies and Reimann]** For any rational  $r$  there is an  $A$  with  $\Sigma_1^0$ -dimension  $r$  s.t. every  $B \leq_{\text{wtt}} A$  has  $\Sigma_1^0$ -dimension  $\leq r$ .

- A set  $A$  is *complex* if there is a computable nondecreasing unbounded  $g$  s.t.

$$C(A \upharpoonright n) \geq g(n).$$

- A set  $A$  is *autocomplex* if there is an  $A$ -computable nondecreasing unbounded  $g$  s.t.

$$C(A \upharpoonright n) \geq g(n).$$

- Note that if  $C(A \upharpoonright n) \geq g(n)$  then  $K(A \upharpoonright n) \geq g(n) - O(1)$ .

- **[Kjos-Hanssen, Merkle, and Stephan; Reimann and Slaman]** There is a complex set that does not compute a 1-random set.

- A function  $f$  is *fixed-point free* (fpf) if

$$\forall e (\Phi_e \neq \Phi_{f(e)}),$$

where  $\Phi_e$  is the  $e$ th partial computable function.

- **[Kjos-Hanssen, Merkle, and Stephan]**

A set is complex iff it (w)tt-computes an fpf function.

A set is autocomplex iff it computes an fpf function.

A c.e. set is wtt-complete iff it is complex.

A c.e. set is (Turing) complete iff it is autocomplex.

- Thus A c.e. set is (wtt-) complete iff it (wtt-) computes an fpf function. **[Arslanov's Completeness Criterion]**

- A  $\Pi_1^0$  class is the collection of paths on a computable binary tree.
- A set is *ranked* if it belongs to some countable  $\Pi_1^0$  class.
- [Chisholm, Chubb, Harizanov, Jockusch, McNicholls, and Pingrey] If  $A \geq_{\text{wtt}} \emptyset'$ , then  $A$  is not ranked.

In fact, every  $\Pi_1^0$  class containing  $A$  has a perfect  $\Pi_1^0$  subclass.

- This result has a simple proof using complex sets.
- If  $\mathcal{P}$  is a  $\Pi_1^0$  class with a complex element  $A$ , then  $\mathcal{P}$  has a perfect  $\Pi_1^0$  subclass.
- So if  $A$  wtt-computes a fpf function then  $A$  is not ranked, and in fact every  $\Pi_1^0$  class containing  $A$  has a perfect  $\Pi_1^0$  subclass.