

*Algorithmic Randomness: Open Questions and New  
Directions*

Rod Downey  
Victoria University  
Wellington  
New Zealand

Notre Dame, May 2010

# THANKS

- Support from the University of Chicago.
- Supported by the Marsden Fund of New Zealand.
- Support from the FRG Grant.
- Correspondences about this topic with Allender, Bienvenu, Gács, Greenberg, Hirschfeldt, Kjos-Hanssen, Merkle, Nies, and others I have forgot.

## REFERENCES

- Calibrating randomness, with Hirschfeldt, Nies and Terwijn, BSL.
- *Algorithmic Randomness and Complexity*, (with Denis Hirschfeldt) to appear Springer Verlag, 2010. (810pp)
- Randomness and computability: Open questions (Nies and Miller). Bull. Symb. Logic. 12 no 3 (2006) 390-410.
- *Computability and Randomness* Nies, OUP, 2009.
- Circuit complexity, Kolmogorov complexity and prospects for lower bounds, Eric Allender, DFCS, 2008.

# PHILOSOPHY

- In every conference, someone draws the short straw, and this time it is me.
- What I plan to do is to try to divide into what I see as questions and directions as follows.
- Technical
- Philosophical
- Synergistic
- Speculative.
- **Also**, I have tried to avoid the problem lists such as the one from Palo Alto maintained by Rebecca Weber <http://www.math.dartmouth.edu/~frg/> or Jack Lutz' home page, which have very fine problems. I have tried to concentrated on things mostly not there, especially ones I have some idea about what the relevant problem means. Please go there for lots of nice problems.

## BASIC CONCEPTS

- We have *many* different Kolmogorov complexities of strings.  $Q \in \{C, K, Km, KM, Km_D, Km_S\}$  (where  $Km_D$  is discrete process complexity and  $Km_S$  is strict process complexity,  $Km_Q$  is quick process complexity, as well as Loveland's decision complexity and others I don't know about).
- A process machine is continuous  $\sigma \prec \tau$  implies  $M(\sigma) \preceq M(\tau)$  if they both halt. This is quick if it is total and there is an order  $h$  such that  $\forall \tau (|M(\tau)| > h(|\tau|))$ .
- Just in case you think these concepts are not central like  $K$  and  $C$ :
- Reimann has established the precise strength of the pointwise *Frostman's Lemma* (and gave a new proof) by looking at *strongly* complex sets where  $A$  is strongly complex if  $KM(A \upharpoonright n) > h(n)$  for some computable order  $h$ . Day shows that *computable* randomness can be characterized by  $A$  is computably random iff for all quick (strict) process machines  $Km_Q^M(A \upharpoonright n) >^+ n$ . (also gets a *tt*-characterization for free.)

- The following seems basic:

## QUESTION

What are the precise relationships between the various  $Q \in \{C, K, Km, KM, Km_D, Km_S\}$  (and others). Only really precise for  $C$  vs  $K$  (Solovay), and kind of close for  $Km$  vs  $KM$ . (Day). Otherwise only upper bounds known.

- Solovay  $K(\sigma) = C(\sigma) + C(C(\sigma)) + C(C(C(\sigma)))$  and the  $C^3$  is sharp.  $KM$  and  $Km$  are within two logs, but it is not known if this is sharp. (Day). Other results can be found in Uspensky and Shen 1996, and Calhoun JSL, and Day's Thesis.
- Such questions are really a bit unpopular (except maybe in moscow) as they are pretty hard, but it would be nice to understand these basic measures.
- Given these other measures the following is natural:

## QUESTION

To what extent can we understand the normal notions of randomness using these other notions of Kolmogorov complexity?

## BIENVENU AND MERKLE'S PROGRAMME

- This also leads to Laurent and Wolfgang's plan of redoing randomness via computable, or even poly-time notions.

### DEFINITION

A function  $f$  with  $\sum_n 2^{-f(n)} < \infty$  is called a **Solovay function** if  $K(n) \leq^+ f(n)$  all  $n$  and  $\exists^\infty n [K(n) =^+ f(n)]$ . This will be computable unless otherwise stated.

- They exist. Consider the machine  $M$  which simulates  $U$  via half its measure, and devotes the other half at  $s$  to  $s$ . Pretend only one change in complexity per stage. If  $n \in \text{ra } U[s]$  drops to  $K_s(n) = m$ , enumerate  $\langle m+1, s \rangle$  into the KC set for  $M$ . This is *Solovay's Solovay Function*.

### THEOREM (HÖLZL, KRÄLING, MERKLE)

*Any time bounded version of  $K$  for superlinear time bound is a Solovay function.*

### DEFINITION (BIENVENU AND MERKLE)

$M$  is a decidable machine iff  $\text{dom } M$  is a computable set.

- Notice that decidable machines correspond more or less to Solovay functions.

### THEOREM (BIENVENU AND MERKLE)

$A$  is MLR iff for all decidable machines  $M$ ,  $K_M(A \upharpoonright n) \geq^+ n$ , iff for all computable  $f$  with  $\sum_n 2^{-f(n)} < \infty$ ,  $f(A \upharpoonright n) >^+ n$ .

### THEOREM (BIENVENU AND DOWNEY)

*f* is a Solovay function iff  $\sum 2^{-f(n)}$  is MLR.

### THEOREM (MILLER AND YU)

*A* is 1-random iff there is a computable function *f* with  $\sum 2^{-f(n)} < \infty$  and  $C(A \upharpoonright n) >^+ n - f(n)$ .

### THEOREM (BIENVENU AND DOWNEY)

Any such *f* is a Solovay function.

### THEOREM (BIENVENU'S "NO GAP")

There is no function *h* tending to infinity with  $K(A \upharpoonright n) >^+ n - h(n)$  implying *A* is MLR (or even Church Stochastic).

### THEOREM (BIENVENU AND DOWNEY, THEN MILLER AND YU)

There is no function *f* tending to infinity (Miller and Yu only ask it be unbounded) with  $K(A \upharpoonright n) \geq^+ n + f(n)$  for all  $A \in \text{MLR}$ .

**THEOREM (BIENVENU AND DOWNEY, THEN IMPROVED BY  
BEINVENU, MERKLE, NIES)**

$K(A \upharpoonright n) \leq f(n)$  iff  $A$  is  $K$ -trivial, for computable (or even upper semicomputable) Solovay  $f$ .

**QUESTION**

Continue this programme. Also for e.g. low Solovay  $f$ . Also the other side. Continue with the Nies, Stephan, Terwijn material on compression functions. Here recall that a compression function  $f$  is one which is a *good lower bound*, e.g.  $f(x) \leq C(x)$ .

**QUESTION**

What about other notions of randomness and dimension and computable approximations? That is, is there some variant of the Solovay function notion relevant for other randomness notions?

## THE USUAL LOWLY SUSPECTS

- There has been a lot of work on lowness. I am sure we have all seen this week:

### THEOREM (MANY, BUT OFTEN NIES)

*The following are equivalent*

- ▶ *A is K-trivial.*
- ▶ *A is low for MLR.*
- ▶ *A is low for K*
- ▶ *A is low for d.c.e. reals*
- ▶ *A is a base of a cone of MLR*
- ▶ *A is low for W2R*

### QUESTION (THE USUAL SUSPECTS)

What about ML non-cuppable? What about ML coverable?

- Not too much progress on these two. One notable recent avenue was by Franklin and Ng. They study randomness for d.c.e. **classes**. So if  $[\sigma] \in V_{i,s}$  and  $[\sigma] \notin V_{i,s+1}$  then no extension of  $\sigma$  is in  $V_i$ .
- When Selwyn showed me this definition, I thought it was just an artifact of the study. But...

### THEOREM (FRANKLIN AND NG)

*The  $\Delta_2^0$  randoms for d.c.e. tests are exactly the incomplete  $\Delta_2^0$  MLR's.*

- Clearly related to **Demuth randomness**. (These are Solovay tests which are c.e. but whose *name* is  $\omega$ -c.e. in the sense that  $V_i = \lim_s V_{f(i,s)}$ ,  $f$  computable and  $f(i, s + 1) \neq f(i, s)$  only  $\leq g(i)$  time for computable  $g$ .)

## QUESTION

Investigate further Demuth-type randomness. Are the only low for Demuth randomness reals computable?

- Downey and Ng have shown that low for Demuth are all hyperimmune-free. Hirschfeldt, Miller, Ng, Nies (CiE) have results on Demuth type randomness.
- By the way thinking of hyperimmune free:

## QUESTION

Is it true that  $\mathbf{0} < \mathbf{b} \leq \mathbf{a}$  implies  $\mathbf{b}$  random is equivalent to  $\mathbf{a}$  being random and hyperimmune-free?

## WHY DO WE CARE?

- Lets concentrate on lowness.

### QUESTION

Why is this interesting? (It is to me, but it is worth asking why in the broader mathematical picture.)

- For example, Slaman and Solovay proved the following amazing result:

### THEOREM (SLAMAN AND SOLOVAY)

*A is low for EX-learning iff A is 1-generic and low.*

- Why has this not also developed a cottage industry around it?
- The first answer (and likely mine) is that our intuition tells us that anything with such apparent depth and interrelationships between what seem *fundamental* concepts *must* be important.
- low things are close to the basic notion of being computable.

- Derandomization power and initial segment complexity seem natural.
- Derandomization clearly leads to  $LR$ -degrees. Lots of nice work here by Barmpalias, Lewis, Miller, Kjos-Hanssen, Yu, and others. Many questions remain. Notable:

### QUESTION

Is there a minimal  $LR$ -degree. Characterize the  $LR$  degrees with countable cones below them. More broadly, how do the  $LR$  and  $T$  or  $tt$  degrees interrelate?

- Perhaps the Barmpalias method of “vaguely multiple permitting” used to prove no minimal pairs of  $\Delta_2^0$   $LR$ -degrees will be a mainstay.

## A WILDLY SPECULATIVE QUESTION

- Already we have seen that certain degree classes align to randomness notions. For example Kummer showed that the c.e. degrees with c.e. sets such that  $\exists^\infty n[C(A \upharpoonright n) \geq^+ 2 \log n]$  are exactly the anc degrees.
- These degrees also align to those of high packing dimension. (Downey-Greenberg)
- These is a randomness notion for the “totally  $\omega$ -c.e. degrees”

### QUESTION

What degree classes can be characterized by randomness notions (however unnatural)? What about  $tt$ -degrees?

- Think of the result that all the double jump classes are definable in the degrees. (Nies, Shore, Slaman)
- Also compare with early work relating MLR and the definability of  $0'$  by Kučera. (“The role of...”)

## A WIDER PERSPECTIVE

- The lowness material has given rise to broader endeavours.
- Two such endeavours are **cost function calculus** and **tracing**.
- Already we have had talks on tracing.

## TRACING

- The idea is that we have some noncomputable object that is close to being computable in the sense that definable aspects of it can be **traced** with a small number of possibilities.
- For example  $A$  is hyperimmune-free iff for all  $f \leq_T A$  there is a computable  $g$  with  $f(n) \leq g(n)$ . So  $f(n) \in \{0, \dots, g(n)\}$ . (Miller and Martin, 60's)
- For example,  $A$  is  $\text{low}_2$  iff there is a function  $f \leq_T \emptyset'$  such that for all  $g \leq_T A$ ,  $g(n) \leq f(n)$  for almost all  $n$ . (Martin)

### DEFINITION (TERWIJN AND ZAMBELLA)

$A$  is **computably traceable** iff there is a computable  $g$  such that for each  $f \leq_T A$ , there exists  $D_{h(n)} = T^n$ , a computable collection of canonical finite sets, with  $f \in T^n$  and  $|T^n| < g(n)$ .

## THEOREM (TERWIJN AND ZAMBELLA)

*A is low for Schnorr null tests iff A is computably traceable.*

- Later extended to Schnorr randomness by Kjos-Hanssen, Nies and Stephan, via Bedregal and Nies.

## TRACING CONTINUED

- In some sense it is kind of clear that tracing should have some thing to do with Kolmogorov complexity. It takes a small number of bits to generate the trace, and then to specify  $f$  (whatever  $f$  is) you only need to say which member of the trace we are dealing with.
- Lots of other notions of tracing. E.g. **computably enumerable** tracing we trace into c.e. sets rather than canonical finite sets. Also **infinitely often** tracing.
- For example  $A$  is called *complex* if  $C(A \upharpoonright n) > h(n)$  for a computable order  $h$  and *autocomplex* iff the same is true for the order  $A$ -computable.

### THEOREM (KJOS-HANSEN, MERKLE, STEPHAN)

*$A$  is autocomplex iff  $A$  is DNC iff  $A$  avoids c.e. traces in the sense that it is not infinitely often c.e. traceable.*

- For the most self-contained proofs and lots of results on i.o. traceability I recommend a recent paper called **Traceable sets** by Hölzl and Merkle.

## QUESTION

Try to understand tracing further. What about moving away from c.e. and computable traces to more general, but vaguely low complexity ones.

## QUESTION (FOR THOSE WHO LIKE SPECIFICS)

The c.e. Turing degrees that have packing dimension 1 are exactly the c.e. non-traceable ones. (Downey and Greenberg) What about the non-c.e. degrees or even the  $\Delta_2^0$  ones? Downey and Ng have shown that c.e. traceability is not enough, nor is array computability.

## QUESTION

Ismukhametov showed that a c.e. degree has a strong minimal cover iff it is c.e. traceable. This is **not** true for  $\Delta_2^0$  degrees. But is there some tracing type characterization maybe solving the old question of whether all minimal degrees have strong minimal covers. Lewis has the state of the art here.

## WHILST WE ARE MENTIONING DIMENSION HERE

- Recall effective packing dimension is  $\limsup \frac{K(A \upharpoonright n)}{n}$  and Hausdorff is  $\liminf$ .

### THEOREM (FORTNOW, HITCHCOCK, ADURI, VINOCHANDRAN, WANG)

*Exponential (and hence tt- or Turing) degrees either have packing dimension 0 or 1.*

### THEOREM (MILLER)

*There are Turing degrees of effective Hausdorff dimension  $0 < a < 1$ .*

### THEOREM (CONDIS)

*There is a Turing degree of effective packing dimension 1 without any real of effective packing dimension 1.*

## QUESTION

Is this true for Hausdorff dimension? ( $\dim_H(\mathbf{a}) = 1$ , and no real of packing dim 1?)

## QUESTION

Where are the Miller degrees? Greenberg and Miller have a minimal degree of effective Hausdorff dimension 1. Where are these degrees? Are these two constructions compatible? What about the situation for strong reducibilities?

## QUESTION

What about lowness for dimension?

- Using work relating to mutual information and a question (later) of Levin, Hirschfeldt, Reimann and Weber have given an alternative proof of Miller's result that there are reals low for effective Hausdorff dimension. This connection cannot be accidental. Much waits to be done here. Also related here is recent work of Lempp, Miller, Ng, Turetsky, Weber on low for dimension.

## SHIFT COMPLEX SETS

- A fascinating recent construction centres around sequences that avoid strings (especially of low complexity).

### DEFINITION

$A$  is called  $\delta$ -shift complex (for  $\delta < 1$ ) if there is a  $d$  such that for all  $n < m$ ,

$$K(A \upharpoonright_n^m) > \delta(n - m) - d.$$

### THEOREM (DURANT, LEVIN, SHEN; MILLER)

*They exist for all  $\delta < 1$ .*

- In some sense this points out a very big difference between dimension and randomness. Usually we think of a real of dimension  $\delta$  as kind of a random real gone to seed. But of course **no** random real can be shift complex since it must have segments of low complexity.
- The best proof is due to Joe Miller (“Two notes on subshifts”).

## MORE ON SHIFT COMPLEX SETS

- Miller's proof is a corollary to the following result.

### THEOREM (MILLER)

*Let  $S \subset 2^{<\omega}$ . Suppose that there is a  $c \in (\frac{1}{2}, 1)$  with  $\sum_{\tau \in S} c^{|\tau|} \leq 2c - 1$ , then there is  $X \in 2^\omega$  avoiding  $S$ , in the sense that no segment in  $S$ .*

- This is applied to  $S = \{\tau : K(\tau) \leq d|\tau| - b\}$ , where  $d \in (0, 1)$ ,  $b = -\log(1 - d) + 1$  and  $c = 2^{-d}$ .

### QUESTION

What about the degrees etc of such objects? They are evidently closed upwards but anything else?

- Here's a specific example:

## QUESTION (KACH)

Suppose that  $A$  is  $d$ -shift complex. Does this mean that  $A$  has effective Hausdorff dimension  $d$ ?

(No; Miller points out that you can splice in a ML random with a  $d$ -shift complex set and makes its Hausdorff dimension go up. The following more general form is open:

## QUESTION

Can a  $d$ -shift complex set  $A$  **ever** have Hausdorff dimension  $d$ ?, or is the dimension always greater than the shift complexity?

- The problem with them is that dealing with them involves manipulation in measure zero sets, and we lack techniques.
- Incidentally, since we are mentioning dimension, Kjos-Hanssen has shown that if  $A$  has positive Hausdorff dimension then  $A$  is a subset of a MLR set. The following question related to this and to reverse mathematics of Ramsey's Theorem has been open for some time.

## QUESTION

# ERGODIC THEORY

## QUESTION (SIMPSON)

These shift complex are related to ergodic theory especially in the setting of  $\mathbb{Z}$ -sequences. (As can be seen by Miller's proof) They deserve investigation from that point of view. Simpson points out lots of nice connections between computability theory and the theory of shifts.

## DEFINITION

A discrete dynamical system consists of a structure  $\mathcal{X}$  with a map  $T$  from  $\mathcal{X}$  to itself. In ergodic theory,  $\mathcal{X} = (X, \mathcal{B}, \mu)$  a finite measure space and  $T$  is a measure preserving transformation, meaning  $\mu(T^{-1}A) = \mu(A)$  for all  $A \in \mathcal{B}$ .

- In this area if we have some  $f$  in  $L^1(\mathcal{X})$  and consider the actions

$$f(x), f(Tx), f(f(T(x))), \dots$$

We can consider the isometry of  $L^1(\mathcal{X})$  induced by  $f \hat{T} : f \mapsto foT$ .

- For example, the **Birkhoff pointwise ergodic theorem** asserts that the sequence for any  $f \in L^1(\mathcal{X})$ , the sequence  $A_n f$  converges pointwise **almost everywhere**, where

$$A_n f = \frac{1}{n} \sum_{i < n} \hat{T}^i f.$$

- That is,  $A_n f(x)$  denotes the average measurement in the first  $n$  points of the orbit of  $x$ .
- Here I refer to Avigad's most excellent paper "The Metamatics of Ergodic Theory" where he discusses some of the issues and things like the Furstenburg structure theorem of additive combinatorics.

- Reimann has asked many nice questions in this area, and the following is a good programmatic one. (He's writing a BSL paperr on this.)

### QUESTION (REIMANN)

What is a general theory of a pointwise dynamical system? What would be a pointwise analog to closure under shift? What is a pointwise theory of "joinings". This has been introduced by Furstenberg in the classical setting and is now one of the standard methods in the field. We have Van-Lambalgen, but this is only the tip of the iceberg. What if the two sequences are not completely independent or only partially random?

- Reimann comments that this would seem to point at a really fascinating interaction with computability (e.g. the Greenberg-Miller minimal degree, various minimal pair results etc). Furthermore, the theory of the K-trivial provides a great pointwise primitive of what it means to have "no information". It also touches the search for the "right" definition of mutual information

## MORE DIVERSIONS

- Recall the Uspensky-Shen notion of KL randomness. Here we bet on the bits (and maybe not all) in some order. The following question is so well-known that I won't even discuss it.

### QUESTION

Is  $\text{KLR} = \text{MLR}$ ? Is this actually important?

- The best results so far are for **oblivious** notions like permutation and injective randomness and due to Kastermans and Lempp.

### QUESTION

What else can be said about these other notions of randomness? Are they interesting?

### QUESTION

What can be said about notions of KL dimensions?

- Recall how we construct supermartingales from tests. As  $\sigma$  appear in the  $V_k$  we bet more on  $\sigma$ . Notice that we might at some stage bet on  $\sigma_0$  then later more on  $\sigma_1$ . Is this necessary?

### DEFINITION

A **Kastergale** is a c.e. supermartingale where is we every decide to bet more on  $\sigma_i$  then thereafter we are stuck with that decision. A **Hitchgale** is the same but as well the *proportion* we bet is a c.e. function. (Details in DH, **buy the book**)

### QUESTION

Is Kasterman random or Hitchcock random the same as MLR? I regard these as quite important questions as they ask is *any* bias okay?

# RETURNING TO TRACEING

## DEFINITION

$A$  is **jump traceable at order  $h$**  iff any  $A$  partial computable function can be traced with  $|T^n| < h(n)$ .  $A$  is sjt iff  $A$  is jt for all computable orders  $h$ .

## QUESTION

Can we turn randomness into plain old computability theory where we simply try to understand the jump operator?

## THEOREM (NIES)

*$A$  is  $K$ -trivial implies that  $A$  is jump traceable at about order  $n \log n$ .  
(Holzl, Kraling Merkle for  $\sum 2^{g(n)}$  finite is enough.)*

## THEOREM (CHOLAK, DOWNEY, GREENBERG)

*For c.e. sets, if  $A$  is jump traceable at about order  $\sqrt{\log n}$  then  $A$  is  $K$ -trivial. There are  $K$ -trivials which are not jump traceable at order  $\log \log n$ . (Nies analyses the proof and get a better bound in his book  $\sqrt{\log \frac{n}{3}}$ .)*

## QUESTION

Is there a order definition of  $K$ -triviality in terms of computable orders? For example is  $A$   $K$ -trivial iff for all computable orders  $h$  with  $\sum 2^{-h(n)} < \infty$ ,  $A$  is traceable at order  $h$ . (Related work by Barmpalias, Downey, Greenberg, and by Ng)

- There is a characterization by Hölzl, Kräling, Merkle but it uses  $K$  which is kind of a cheat. (Also in this characterization they use  $O$  in the definition, but the  $O$  factor depends on the function.)

# STRONG JUMP TRACEABILITY

## THEOREM (CHOLAK, DOWNEY, GREENBERG)

*The c.e. sjt degrees form an ideal.*

## THEOREM (NG)

*It is  $\Pi_4^0$  complete.*

## THEOREM (DOWNEY AND GREENBERG)

*If  $A$  is sjt there is a  $K$ -trivial c.e.  $B$  with  $A \leq_T B$ .*

## QUESTION

*Is there a sjt  $B$ ? Are they closed under  $\oplus$ ?*

### DEFINITION (NIES)

If  $\mathcal{C}$  is a class of sets,  $\mathcal{C}^\diamond$  is the collection of c.e. sets below all the random members of  $\mathcal{C}$  (which might be empty).

### THEOREM (HIRSCHFELDT; MILLER)

If  $\mathcal{C}$  is a  $\Sigma_3^0$  nullset, then  $\mathcal{C}^\diamond \neq \emptyset$ .

### THEOREM (GREENBERG, HIRSHFELDT, NIES)

$Sjt = (\text{superlow})^\diamond = (\text{superhigh})^\diamond$ .

### QUESTION

Any other such coincidences? Any of those other things like ML cuppable? Coverable etc? What about other random collections of  $\Delta_2^0$  randoms? Are they related to Ng's *hyper jump traceables* (where the orders can grow slower than computable ones).

## QUESTION

Related: Is there a low random degree above all the  $K$ -trivials. Slaman and Kučera have shown that the answer is yes if “random” is removed. Also GHN have results about randoms and sjt’s.

## QUESTION

Is there a Demuth random above each sjt (c.e.) real?

## QUESTION (VAGUELY RELATED)

Is it true that for all  $A$  there is a  $B \not\leq_T A$  with  $A \equiv_K B$ ? (Generalizing the construction of a  $K$ -trivial.) What about asking that if  $A$  is c.e. needing  $B$  also to be c.e..

## COST FUNCTIONS

- Nies abstracted the ideas of the construction of a  $K$ -trivial as one of a cost function. Put  $x$  into  $A$  at  $s$  if it meets  $R_e$  and is  $e$ -cheap.
- The *standard* cost function is  $c(n, s) = \sum_{n \leq i \leq s} 2^{K_s(i)}$ . A set obeys a cost function if it has an enumeration  $A = \lim_s A_s$  where  $\sum \{c(n, s) : n \text{ least at } s \text{ with } A_{s+1}(n) \neq A_s(n)\} \leq \infty$ .
- A metatheorem inspiring all this is the one of Nies.

### THEOREM (NIES)

*A is K trivial iff A obeys the standard cost function.*

- The idea here is to attack problems by setting up a cost function definition of satisfaction and then appealing to a metatheorem. For example

### THEOREM (NIES)

*Suppose that  $Y \leq_T \emptyset'$  is Demuth random and A obeys Y's cost function. Then  $A \leq_T Z$  for every  $\omega$ -c.e. MLR Z and hence by work of Greenberg, Hirschfeldt and Nies, (above) A is sjt.*

## THEOREM (NIES)

*Suppose that  $Y \leq_T \emptyset'$  is Demuth random and  $A$  obeys  $Y$ 's cost function. Then  $A \leq_T Z$  for every  $\omega$ -c.e. MLR  $Z$  and hence by work of Greenberg, Hirschfeldt and Nies, (above)  $A$  is sjt.*

- Recently superceded by

## THEOREM (KUČERA-NIES)

*Suppose that  $Y \leq_T \emptyset'$  is Demuth random and  $A$  is c.e. and  $A \leq_T Y$ . The  $A$  is sjt.*

- Lots of classifying various kinds of cost functions. **monotone benign**, etc

## QUESTION

To what extent is the theory able to be developed on the assumption that e.g. the listing of the cost functions is e.g.  $\Delta_3^0$ , etc?

- Lots of work here and work yet to be done abstracting work both in classical computability and algorithmic randomness.

## INVERSIONS

- Of course, low down corresponds to high up.
- Jockusch-Shore pseudo jump inversion says that if  $V_e$  is a CEA operator and nontrivial then there is a c.e.  $X$  with  $V_e^X \equiv_T \emptyset'$ .
- Ng has recently shown this fails for strong reducibilities.
- apply this to  $V_e=K$ -trivial we get something where  $\emptyset'$  is  $K$ -trivial relative to  $X$ , and similarly if  $V_e$  is sjt,  $\emptyset'$  is ultra-high, meaning that  $\emptyset'$  is sjt relative to  $X$ .
- We know that  $\emptyset'$ -trivializing reals are a.e. dominating. (Cholak, Greenberg, Miller) in the sense that they can compute  $f$  which is a.e. dominating.

### QUESTION (CHOLAK, GREENBERG, MILLER)

Is there a minimal pair of such c.e. sets? The answer is **yes** if c.e. is removed. (Barnali)

- Clearly if c.e.  $A$  is ultra-high (indeed  $\emptyset'$  is  $\sqrt{\log n}$ jt relative to  $A$ ) then it is  $\emptyset'$ -trivializing.

### THEOREM (DOWNEY AND GREENBERG)

*There are no c.e. minimal pair of ultra-high c.e. sets.*

### THEOREM (DOWNEY AND GREENBERG)

*In fact c.e. set  $Z \not\equiv_T \emptyset$  below all of them.*

- this **solves** one and relates to old questions:

### QUESTION

(Downey, Jockusch, LaForte) Is there a CEA operator which does not avoid upper cones? This is related to (Rogers) Is there a degree invariant to Post's Problem? Lewis has the best results to date on the non-uniform (of Rogers' question) case.

## ANOTHER PROGRAMME

- We know that every (nonempty)  $\Pi_1^0$  class has a low member. (Jockusch Soare)
- Generalizing, is it true that every  $\Pi_1^0$  class  $P$  has members of all jumps? Well **no** of course,  $P$  could contain only computable members. Not very **sporting** counterexample.
- Every **special**  $\Pi_1^0$  class has members jumping to any  $X \geq_T \emptyset'$ . (folklore)
- What about  $\Delta_2^0$  members jumping to all possible targets? No, e.g. a thin class. (No!)
- Need further conditions. Having *positive measure* is enough (more or less Kůčera).

### QUESTION (EXTENDED KUČERA PROGRAM)

Investigate the jumps of members of thin and special classes, particularly with respect to things like cone avoidance etc.

- For example Barmpalias, Downey, Ng have proven that any  $X > \emptyset'$  *hyperimmune* wrt  $\emptyset'$  is the jump of of a MLR  $Y$  which forms a minimal pair with  $\emptyset'$ , and hence is W2R.

## QUESTION

What are the possible jumps of W2R's? What about the possible jumps of hyperimmune-free degrees. (old question of Jockusch)

## MUTUAL INFORMATION

- We have a pretty good idea of what mutual information is for  $C$  and  $K$ , e.g.  $I_K(\sigma : \tau) = K(\tau) - K(\tau | \sigma)$ . Many applications of Symmetry of Information and the like.

### QUESTION (LEVIN)

What is the correct notion of mutual information for infinite sequences?

- Levin had suggested

$$I(A : B) = \log \sum_{x,y} m(A \upharpoonright x) m(B \upharpoonright y) \frac{m(x,y)}{m(x)m(y)}$$

where  $m$  is the optimal discrete semimeasure. He also has another notion related to when a real leaves a universal test.

- He points out that any notions which makes  $I(\alpha, \alpha) < \infty$  should happen iff  $\alpha$  is  $K$ -trivial.

## THEOREM (HIRSCHFELDT, REIMANN, WEBER)

*There are reals trivial for these notions of mutual information and yet not  $K$ -trivial.*

- Another desirable thing would be that if  $I(A : B) < \infty$  then the reals should form a LR minimal pair.
- Perhaps there are also other tests which would be desirable.
- I think this is a really important programme.

- Related here is Zimand's work on computational independence.
- $X$  and  $Y$  should be "independent" iff their segments have little in common. For instance
 
$$C((X \upharpoonright m)(Y \upharpoonright n)) \geq C(X \upharpoonright m) + C(Y \upharpoonright m) - O(\log m + \log n).$$
- good enough for many applications.

### THEOREM (ZIMAND)

*If  $X$  and  $Y$  are somewhat random, e.g. have positive Hausdorff dimension, and are independent, then  $X \oplus Y$  tt-computes a real of dimension 1.*

### QUESTION

Investigate. How does this relate to the Miller phenomenon. How does independence in this sense affect the Turing degrees of  $\alpha$  and  $\beta$ . etc.

## OTHER SETTINGS

- Gács, building on older work of Levin has pioneered working on randomness in other spaces outside of Cantor and Baire Space.

### QUESTION (GÁCS)

- (I) What is the "right" kind of notion of randomness, when the probability space is a general constructive metric space?
- (II) what is its connection to the complexity of approximations (like there is one for computable measures over the space of sequences).
- (III) What is the "right" notion of "information" in this context, and its relation to randomness?
- (IV) (Demuth's programme) How are the randomness questions related to constructive issues in measure theory?

- Gács has material on this in his web site, and a recent TCS paper with Hoyrup and Rojas.
- Of course more work needed on computable continuous functions and random sets. (Cenzer, Kjos-Hanssen, Brodhead)

- In the Gács etc papers many of the basic machinery seem to go through.
- This also seems related to the Reimann-Slaman materials on questions asking when reals can be *continuously random*. We have seen a lot on this material and I won't discuss it here. It clearly points at deep connections with set theory and analysis.

## QUESTION

Investigate further.

- It also seems related to The Levin-Gács theory of uniform tests and neutral measure.
- There is recent work by Bienvenu, and by Day and Miller showing the connection between this framework and the more naive computability theoretic approach that used by Kautz, Reimann, Slaman etc. and we can translate between the two.

### QUESTION (REIMANN)

The theory seems a fine tool to bring more sophisticated analytic methods to the field (for example Bienvenu has given a on-line proof that every random closed set contains a random real), while in the other direction it opens the door for computability theoretic methods in other fields such as ergodic theory. Investigate.

### QUESTION

Can we use computability theoretical methods to get alternative proofs of known analytical results? (e.g. Reimann's new proof of Frostman's lemma.)

## DEMUTH'S PROGRAMME

- These are many theorems in classical analysis saying that something happens almost everywhere. Demuth had a programme which said that computable functions should behave well at random points.
- This suggests a programme in computable analysis relating effective randomness and good behaviour.

### THEOREM (BRATTKA, MILLER, NIES)

*A computable function which is monotone on an interval is differentiable at every computably random point. This is sharp. Also (Also **Demuth**) There is a computable continuous real valued function of bounded variation only differentiable at the ML random points.*

### QUESTION

More of the same. How does this relate to Reverse Mathematics? For example, what new principles do we get and how do they interrelate to calibrating strengths of theorems of analysis?

- This relates to Simpson's programme to look at Ergodic theory. Which *as usual* goes back to work of Russians (fortunately actually published! not just the Moscow seminar). (e.g. V'yugin, V. V. Ergodic theorems for individual random sequences. Theoret. Comput. Sci. 207 (1998), etc)
- Hoyrup and Rojas show that one version Ergodic Theorem (in the presence of certain natural assumptions) is equivalent to the existence of Schnorr randoms. It would seem that other Ergodic Theorems likely would be equivalent to e.g. (maybe) W2R.
- Avigad also examines some aspects of Ergodic theory. Points at the connections between this result and the aforementioned Lebesgue theorem noted by Tao on his blog.

## APPLICATIONS

- Also the recent important work by Green and Tao on arithmetical progressions in the primes. We have touched on this when we discussed Ergodic Theory.
- This uses the false assumption that once obvious things are taken away the primes look random.

### QUESTION

Can this be made precise?

- Also the “Dense Model Theorem”. This theorem generalized the Szemerédi proof on arithmetical progressions, saying that, roughly, in big models you get a decomposition of things in randoms and well behaved.
- To wit: If  $R$  is a (possibly very sparse) pseudo-random subset of a set  $X$  (in the sense that every function of low complexity relative to some family  $F$  has approximately the same average on  $R$  as on  $X$ ) and  $D \subseteq R$  containing a noticeable large (say  $\delta$ ) fraction of  $R$ , then there is a large set  $M \subset X$  containing a noticeably large fraction of all the elements of  $X$  and is indistinguishable from  $D$ . (Green, Tao and Ziegler) (see e.g. Trevisan, Tulsiani, Vadhan, CCC 2009)

## QUESTION

Can this be made precise?

## GENERIC CASE COMPLEXITY

- Whilst we are talking about things like Szemerédi's Theorem which concerns positive (upper Banach) density and has connections with ergodic theory, I would like to pont at:
- Kapovich, Myasnikov, Schupp, Shpilrain on algorithmic that run fast and give correct answers with density 1 (which are defined in J Algebra, 264 (2003) 665-649, and explored in JSL and a later Advances paper. For example, almost all finitely presented groupd are hyperbolic, and algorithmically behave well. (also Sela **Come to Wellington, December 2011**)

## QUESTION

This begs for investigation. Of our community only Frank Stephan has made a contribution.

- **Wrong!** As I found out last week, Jockuch and Schupp are actively exploring the computability theory. It presents unique challenges.
- Also Kapovich and Schupp *On Group Theoretical Models of Randomness and Genericity and Some Quantitative Aspects of Fractional Computability.*

see

<http://www.math.uiuc.edu/~kapovich/research.html>

## QUESTION

What about physics?

- Gács, then Kjos-Hanssen and Nerode, and Tadaki have made some heroic efforts here notable in Thermodynamics, Brownian motion. Tadaki has a very interesting programme here. What about the Quantum stuff?

## QUESTION

What about biology?

- Things like evolution, mutual information. Has been used for evolution of music (Vitanyi and others).

## QUESTION

What about MCMC? (Markov Chain Monte Carlo) This is the most important area of applied statistics of the 21st and late 20th century. Can our results talk to this methodology?

## QUESTION (SPECULATIVE)

Is Kolmogorov complexity a reasonable parameter to fix for understanding (finite) or countable model theory? **Buy the other book!**  
(Sorry Andre: I mean *Parameterized Complexity*)

## MORE DIVERSIONS

- You might ask, how could you use  $I(\sigma, \tau)$  for mutual information in applications when  $C$  and  $K$  are noncomputable? Answer: approximate.
- Applications can use GZIP, which in turn uses Lempel-Ziv.

### QUESTION

Continue the work of Lutz, Hitchcock etc to understand low complexity compression, martingales and the like.

- I refer the reader to Lutz' site where there's a list of questions.
- Here's one I have tried without success to solve.

### QUESTION (THE ONE BIT CATASTROPHE-LUTZ)

Is there a sequence  $A$  which is LZ-incompressible, yet  $0A$  is highly compressible?

- Lutz, Hitchcock, Mayordomo etc have related measures in the miniature to questions in complexity, via things like the *Small Span Theorem*. Basically, if we assume  $NP \neq P$  for instance, you can ask how big e.g. the collection of NP complete sets are in NP.
- This brings us to complexity theory:

## SOME SYNERGISTIC QUESTIONS WRT COMPLEXITY

- The use of randomized algorithms and their relationship with complexity classes is the hottest topic in complexity and has been for 10 years or more.
- Here are just some directions our work might impact if we work towards that.

## THE COLLECTIONS OF (NON-)RANDOM STRINGS AND OVERGRAPHS

- Pick a Kolmogorov complexity  $Q$ . Then look at  $R_Q = \{\sigma : Q(\sigma) \text{ is big enough to be random, or maybe half random}\}$ . And also the overgraph being  $O_R = \{(\sigma, n) \mid Q(\sigma) \leq n\}$ .
- These are natural c.e. or co-c.e. sets.
- For example, if  $Q = C$ , then  $R_C$  is evidently wtt complete. (Use the Recursion Theorem to control, for each  $n$ , all the strings of length  $f(n)$ . At any stage point at the leftmost string  $\tau_{f(n),s}$  of this length currently random and if  $n$  enters  $\emptyset'[s]$ , make  $\tau_{f(n),s}$  non-random at  $s + 1$ .)
- The question is : What about more constrained reductions to  $R_C$ ?

- Long ago Kummer showed that  $R_C$  is **truth table** complete. The reduction is double exponential and moreover, nonuniform. It is a disjunctive truth table reduction, and Allender, Buhrman and Koucký in (2006 APAL) showed no such dtt-reduction could be performed in less than exponential time.
- Allender and his co-workers have pursued a programme of seeing what is *efficiently* reducible to such sets.

### QUESTION (ALLENDER)

Is  $\emptyset' \in P^{R_C}$ ?

- Answers often depend on choice of universal machine.

## QUESTION

Does the answer depend on the choice of universal machine?

- The first example of such a dependence this was Muchnik's Theorem:

## THEOREM (MUCHNIK, APAL)

*There exist universal (by adjugation) prefix-free machines  $M_1$  and  $M_2$  with*

- (i)  $K_{M_1}$  tt-complete, and*
- (ii)  $K_{M_2}$  not tt-complete.*

- The proof of (ii) is extremely interesting as it uses determinacy of finite games. That is, to defeat a *tt*-reduction  $\Gamma$  via some witness  $n$ , the opponent has under its control, the ability to lower the complexity of some strings whose length is  $\leq \gamma(n)$ , and so do we. To decide whether to put  $n$  into some diagonal set  $D$ , play the winning strategy. Muchnik's technique has other applications and maybe a lot more in the area.

## COMMENTS

- These have analogs for other complexity measures.

### THEOREM (ALLENDER, BUHRMAN, KOUCKÝ, ALSO DAY)

*For any of  $Q \in \{C, K, Km, KM, Km_D, Km_S\}$  (where  $Km_D$  is discrete process complexity and  $Km_S$  is strict process complexity), there is a universal machine where the set of non-random strings wrt  $Q$  is  $tt$ -complete.*

### THEOREM (DAY)

*For any universal monotone machine the overgraph is  $tt$ -complete. The same is true for  $KM, Km_D, Km_S$ .*

- Day's Theorem is  $\emptyset'$ -nonuniform, whereas Kummer's is  $\emptyset''$ . Is this necessary for Kummer's Theorem?

## THEOREM (DAY)

*There is a universal strict process machine where the non-randoms aren't tt-complete.*

## QUESTION

What about the other Kolmogorov complexities?

## AND HOW DOES THIS RELATE TO COMPLEXITY?

- $EXP = 2^{poly} = \cup_k DTMIE(n^k)$ , and  $NEXP = \cup_k NTIME(n^k)$ .

### THEOREM (ALLENDER ET. AL)

For any choice of universal machine  
 $PSPACE \subseteq P^{R_C}$  and  $NEXP \subseteq NP^{R_C}$ .

### QUESTION

Find a nice proof of these. The current proofs use very sophisticated machinery from derandomization results and interactive proofs.

### QUESTION

Could it be that  $PSPACE = \cap \text{Universal } M P^{R_C^M}$ ?

### QUESTION

Allender, Koucký, Ronnenburger and Roy exhibit a  $P/Poly$  reduction from  $\emptyset'$  to  $R_C$ . Allender asks if the nonuniformity is essential? (Recall  $P/Poly$  is the class which is poly time with poly size advice.)

- Much of the current work in complexity centres around  $P/poly$ . Recall that this is the class of languages with *poly sized circuits*.
- On input of length  $n$ , you have a advice of size  $n^k$ , and with that can solve the problem in poly time.
- Early on circuit complexity had real advances.

### THEOREM (RAZBOROV, AJTAI, ETC)

*Various NP problems cannot have monotone or fixed depth poly circuits.*

- For fixed depth, the proof can work by induction on the depth. Want to invert the top layer of “OR of ANDS” into “AND of ORS” and coalesce. The switching lemma shows that for random assignation of a relatively small number of variables, this is possible and is also why non-uniformity is needed.
- The switching lemma has been proven using Kolmogorov complexity to replace the probabilistic arguments.

- Actually a lot of results in complexity can be/have been obtained using Kolmogorov complexity. (Li, Vitanyi, Fortnow, Laplante, Maass, etc)
- Unfortunately, things in  $P$  like PARITY don't have constant depth circuits, and then the *natural proof* results of Razborov and Rudich dampened enthusiasm. (Similarly the recent *algebraization* results of Wigderson and his co-workers.)
- Allender (references) points out a possible way round these obstacles.
- A wonderful theorem you should know here is the following.

### THEOREM (IMPAGLIAZZO AND WIGDERSON)

*If NP needs more or less exponential circuits, then  $BPP = P$ . That is, if NP is as hard as we think, then every randomized algorithm in BPP can be derandomized.*

- We need to learn the material on derandomization, extractors etc.

## A CONNECTION

- Define  $SIZE(f)$  to be the size of the smallest circuit computing  $f$ , where  $f$  is a boolean function on  $n$  variables for some  $n$ . (can easily be extended to strings as functions).

**THEOREM (ALLENDER, BUHRMAN, KOUCKÝ, VAN MELKEBEEK, RONNEBURGER, 2006)**

$$C(\sigma) = SIZE^{\Theta}(\sigma).$$

- There are various time bounded versions of  $K$ . For example Levin's  $Kt(\sigma) = \min\{|\tau| + \log t : U(\tau) = \sigma \text{ in time } t\}$ .

**THEOREM (ALLENDER, BUHRMAN, KOUCKÝ, VAN MELKEBEEK, RONNEBURGER, 2006)**

- (I) If  $A$  is complete for  $E(= DTIME(2^{O(n)}))$ , then  $Kt(\sigma) = SIZE^A(\sigma)$ .
- (II)  $EXP = NP^{R_{Kt}}$  and  $R_{Kt}$  is complete for  $EXP$  under  $P/Poly$  reductions.
- (III)  $R_{Kt}$  is **not** complete for  $EXP$  under poly time truth table reductions.

# THE MOST IMPORTANT QUESTION OF THE FIELD

## QUESTION

When will you buy “the book”?

- Cheaper in bulk.
- Very reasonably priced.
- Make excellent Christmas presents, superb doorstops.
- Make excellent pets.

Thank you