# AIM/ARCC Workshop in Effective Randomness
August 7–11, 2006
Open Problem List – **updated (live) version**
Last updated: December 17, 2007

## 1. Introduction

This is the open problem list for the AIM workshop in Effective Randomness organized by Hirschfeldt and Miller, held at ARCC, Palo Alto, CA, Aug 7–11, 2006. It is intended to be self-contained regarding definitions, but contains no proofs. There is nontrivial overlap between this list and that of Miller and Nies, though each contains many questions not in the other. In particular, this list contains many "soft" questions, those which are not answerable by "yes" or "no".

1.1. **Conference participant interest summary.** Computability (recursion) theory has been applied to solve problems in randomness, as well as simply to find workable definitions of randomness. Problems in randomness, conversely, have led to new proof techniques, examples, and questions in computability, as well as results related to Turing degrees and other well-established elements of traditional computability theory. What additional connections can be found, particularly in the randomness-to-computability direction? Going further, what connections (additional to those already known) can be found between randomness and set theory, mass problems, reverse mathematics, effective dimension, information theory, computable analysis, and mathematics at large? How do we extend the notion of randomness to sets and functions? What is the right way to compare the randomness of different real numbers? And finally, how can our study of abstract randomness be applied to the practical question of pseudo-random number generation?

1.2. **Notation.** Different traditions give varying notation for the same concepts. For countable infinity, $\infty$, $\omega$, and $\mathbb{N}$ are used. As a superscript $X^\omega$ they indicate the set of infinite strings on the alphabet $X$. The set of finite strings on $X$ is indicated by $X^{<\omega}$ (et al.) or $X^*$. When $\{0, 1, \ldots, k-1\}$ is playing the role of $X$ it may be abbreviated to $k$.

For an infinite sequence $\alpha$, $\alpha \upharpoonright n$ means the restriction to the length-$n$ initial segment of $\alpha$, or in other words to $\alpha[0]\alpha[1]\ldots\alpha[n-1]$. When $\sigma$ is a finite string and $\rho$ is either finite or infinite, $\sigma \subseteq \rho$ means $\sigma$ is an initial segment of $\rho$. Concatenation of $\sigma$ and $\tau$ is denoted $\sigma^\frown\tau$ or simply $\sigma\tau$. The *join* of two infinite strings, $A \oplus B$, is the interleaving of their bits. In terms of sets, $A \oplus B = \{2n : n \in A\} \cup \{2n+1 : n \in B\}$.

The notation $+c$ or $+\mathcal{O}(1)$ will always mean a constant independent of the input.

Measure $\mu$ used without specification means Lebesgue measure; on the binary tree this is the coin-toss probability measure.

1.3. **Definitions used throughout.** We begin with few basic definitions. By *real* we mean an element of $2^\omega$. A *computable real* is one which is the characteristic function of a computable set. A *c.e. real*, however, is the limit of a computably increasing sequence of rationals. This is also called *left c.e.*, to distinguish it better from *strongly c.e.* reals, those which are the characteristic function of a c.e. set.

A *truth table* is a Boolean combination of finitely-many variables $x_i$; they may be computably enumerated. A set $X$ *satisfies* the truth table if, interpreting $i \in X$ as $x_i$ and $i \notin X$ as $\neg x_i$, the Boolean combination is true for $X$. $A$ is *truth-table*

*reducible* (tt-reducible) to $B$, $A \leq_{tt} B$, if there is a computable function $f$ such that $n \in A$ if and only if $B$ satisfies the $f(n)^{th}$ truth table.

The three major approaches to randomness are through statistical tests, compression, and betting.

**Definition 1.1.** A *Martin-Löf test* is a sequence $\{U_i\}_{i\in\omega}$ of uniformly c.e. open classes (uniformly $\Sigma^0_1$ classes) such that $\mu(U_i) \leq 2^{-i}$ for all $i$.

A real $X$ *passes* the test if $X \notin \bigcap_i U_i$.

There is a *universal* Martin-Löf test, a $\{U_i\}$ such that $X$ passes $\{U_i\}$ if and only if it passes all Martin-Löf tests.

**Definition 1.2.** A set of strings $\{\sigma_i\}_{i\in I}$ is *prefix-free* if $\sigma_i \subseteq \sigma_j$ implies $\sigma_i = \sigma_j$.

A Turing machine if *prefix-free* if its domain is.

There is a universal prefix-free Turing machine: one that can simulate all other prefix-free machines.

**Definition 1.3.** The *prefix-free Kolmogorov complexity* of a finite string $\sigma$ *relative to machine* $M$ is $K_M(\sigma) = \min\{|p| : M(p) = \sigma\}$.

The prefix-free complexity of $\sigma$ is $K(\sigma) = K^U(\sigma)$, where $U$ is a universal prefix-free Turing machine.

If we do not require the machines be prefix-free, but allow arbitrary Turing machines, we obtain analogously the concept of *plain Kolmogorov complexity*, $C(\sigma)$.

**Definition 1.4.** A *martingale* is a function $d : 2^{<\omega} \to [0, \infty)$ such that for all $\sigma \in 2^{<\omega}$, $d(\sigma) = \frac{1}{2}(d(\sigma 0) + d(\sigma 1))$. That is, it represents fair double-or-nothing betting on the bits of a string.

The martingale $d$ *succeeds* on an infinite string $X$ if $\limsup_{n\to\infty} d(X \upharpoonright n) = \infty$.

**Definition 1.5.** A martingale is *computably enumerable* (*constructive*, *effective*) if it is lower semi-computable (effectively approximable from below); that is, there is a computable function $\hat{d} : 2^{<\omega} \times \omega \to [0, \infty)$ such that for all $\sigma \in 2^{<\omega}$, $t \in \omega$, $\hat{d}(\sigma, t) \leq \hat{d}(\sigma, t + 1) < d(\sigma)$ and $\lim_{t\to\infty} \hat{d}(\sigma, t) = d(\sigma)$.

There is a universal c.e. martingale, just as with Martin-Löf tests. However, there is no *optimal* martingale; that is, c.e. $f$ such that for each c.e. martingale $g$, $(\exists c)(\forall\sigma)[cf(\sigma) \geq g(\sigma)]$. To obtain an optimal (universal) betting strategy requires we use *supermartingales*, for which Definitions 1.4 and 1.5 carry over but with the inequality $d(\sigma) \geq \frac{1}{2}(d(\sigma 0) + d(\sigma 1))$ in place of the equality in 1.4. In terms of defining randomness, supermartingales are equivalent to martingales.

**Definition 1.6.** To say a real $X$ is 1-*random* means it has the following equivalent characteristics:

(i) $X$ passes the universal Martin-Löf test.
(ii) $(\exists c)(\forall n)[K(X \upharpoonright n) \geq n - c]$.
(iii) The universal c.e. (super-)martingale does not succeed on $X$.

1-random is also commonly called ML-random.

"Random" used without qualification means 1-random.

## 2. Effective Dimension

The problems in this section deal with effectivizations of Hausdorff and packing dimension. To define classical Hausdorff dimension, $\dim_H$, for a set $X$, let $\mathcal{A}^\delta$ be the collection of all sequences $\{A_i\}$ that cover $X$ by balls of diameter $\leq \delta$. The *Hausdorff outer measure of dimension s* is

$$H^s(X) = \lim_{\delta \to 0} \left( \inf_{\{A_i\} \in \mathcal{A}^\delta} \left\{ \sum_{i=1}^{\infty} \operatorname{diam}(A_i)^s \right\} \right).$$

$H^s(X)$ will be $\infty$ for lower values of $s$ and 0 for higher, with at most one point in between which is neither 0 nor $\infty$. The location of that change is the Hausdorff dimension of $X$: $\dim_H(X) = \inf\{s : H^s(X) = 0\} = \sup\{s : H^s(X) = \infty\}$.

Classical packing dimension, $\dim_p$, is dual to Hausdorff dimension. Instead of covering $X$ by balls of a given radius we pack it with disjoint balls of that radius. An extra step must be taken in creating the outer measure, but once that is established the definition of dimension from the measure is the same.

Three books are suggested reading: *Hausdorff Measures* by C.A. Rogers, *Fractal Geometry* by K. Falconer, and *Geometry of Sets and Measures in Euclidean Space* by P. Mattila.

**Definition 2.1.** An *s-gale* is a function $d : \Sigma^* \to [0, \infty)$ such that for all $w \in \Sigma^*$,

$$d(w)\mu(w)^s = \sum_{a \in \Sigma} d(wa)\mu(wa)^s,$$

where $\mu(w) = |\Sigma|^{-|w|}$ and $wa$ is $w$ concatenated with $a$.

A martingale is thus a 1-gale over the alphabet $\{0, 1\}$. Constructive $s$-gales are defined just as for martingales.

**Definition 2.2.** The $s$-gale $d$ *succeeds* on a string $X$, denoted $X \in S^\infty[d]$, if

$$\limsup_{n \to \infty} d(X \upharpoonright n) = \infty.$$

It *succeeds strongly*, $X \in S^\infty_{str}[d]$, if lim sup above may be replaced by lim inf.

The dimension of a string is a measure of the most hostile environment (least $s$) in which an $s$-gale succeeds on the string.

**Definition 2.3.** The *constructive dimension* of a sequence $X \in \Sigma^\infty$ is

$$\operatorname{cdim}(X) = \inf\{s : \exists \text{ a constructive } s\text{-gale } d \text{ such that } X \subseteq S^\infty[d]\}.$$

The *constructive strong dimension* of $X$ is

$$\operatorname{cDim}(X) = \inf\{s : \exists \text{ a constructive } s\text{-gale } d \text{ such that } X \subseteq S^\infty_{str}[d]\}.$$

Constructive dimension is an effectivization of Hausdorff dimension, and is also referred to as effective dimension or effective Hausdorff dimension. Constructive strong dimension is an effectivization of packing dimension.

The first question about effectivized dimension is its relationship to the classical version. Lutz uses the term *correspondence principle* for an effective dimension theorem defining a class of examples on which constructive measure coincides with classical measure. Hitchcock (2002) proved that if $X \subseteq \Sigma^\infty$, $\Sigma$ a finite alphabet, is a (not necessarily effective) union of $\Pi^0_1$ classes, then $\operatorname{cdim}(X) = \dim_H(X)$.

**Problem 2.4.** (Lutz.) What is the correspondence principle for constructive strong dimension, cDim?

Problem 2.4 is one of a family of similar problems. We may generalize $s$-gales to $\nu$-$s$-gales, where the metric induced by the uniform probability measure $\mu$ on $\Sigma^*$ is replaced by the metric induced by any strongly positive (Borel) probability measure $\nu : \Sigma^* \to [0,1]$ (Lutz and Mayordomo, 2006). The dimensions $\mathrm{cdim}^\nu$ and $\mathrm{cDim}^\nu$ are then defined in the natural way. What correspondence principles may be obtained in the general situation?

A different generalization would be the following.

**Problem 2.5.** (Reimann.) Viewing constructive dimension as an effectivization of Hausdorff dimension, we might refer to it as $\Sigma^0_1$-H-dim. Can we make a productive definition for $\Sigma^0_n$-H-dim?

Computable reals all have constructive dimension 0, and random reals have constructive dimension 1. J. Miller conjectures the following questions about reals of dimension $> 0$ all have negative answers.

**Problem 2.6.**
(1) If $\mathrm{cdim}(X) > 0$, does $X$ compute a real of higher dimension? Arbitrarily high dimension $< 1$? Dimension 1?
(2) If $\mathrm{cdim}(X) > 0$, does $X$ compute a random real? If $\mathrm{cdim}(X) = 1$?

**Update.** Bienvenu, Doty, and Stephan proved that for any $A$, if $\varepsilon > 0$ and $\mathrm{cDim}(A) > 0$, then $A$ wtt-computes some $B$ such that $\mathrm{cdim}(B) \geq \frac{\mathrm{cdim}(A)}{\mathrm{cDim}(A)} - \varepsilon$. At the Sept 2007 workshop Joe Miller announced a negative answer to Problem 2.6: for all rational $\alpha \in (0,1)$ there is a sequence $A$ such that $\mathrm{cdim}(A) = \alpha$ and for all $B \leq_T A$ $\mathrm{cdim}(B) \leq \alpha$. He believes his technique will work with modification for irrational dimensions as well.

Define the dimension of a set of reals (e.g., a Turing degree) to be the supremum of the dimensions of all reals in that set. In the wtt- (and hence tt-) degrees, there is a degree of intermediate constructive dimension, strictly between 0 and 1.

**Problem 2.7.** (Reimann, Terwijn.) Is there a Turing degree of intermediate constructive dimension?

There are several examples of reals $X$ of non-integer effective dimension whose Turing lower cones $\{Y : Y \leq_T X\}$ have effective dimension 1. First, a Hölder transformation of the Cantor set: $X_r(m) = X(n)$ if $m = \lfloor n/r \rfloor$ and 0 otherwise, for some rational $0 < r < 1$ and 1-random $X$. While $\mathrm{cdim}(X_r) = r$, it is clear $X$ may be extracted from $X_r$, and hence $X_r$'s Turing lower cone has effective dimension 1.

Next, take $X$ random with respect to the Bernoulli measure $\mu_p$, bias $p \in \mathbb{Q} \cap [0,1]$. In this case $\mathrm{cdim}(X)$ is the entropy of $\mu_p$, $H(\mu_p) = -[p \log p + (1-p)\log(1-p)]$ (where log is $\log_2$ in Cantor space). $X$ computes a 1-random real $Y$ by von Neumann's trick: take $X$ two bits at a time, discard them if they are the same, and add the first to the initial segment of $Y$ if they are different.

Finally, alter Chaitin's $\Omega$ by letting $\Omega^{(s)} = \sum_{\sigma \in \mathrm{dom}(U)} 2^{-|\sigma|/s}$, where $U$ is a universal prefix-free Turing machine and $0 < s \leq 1$ is a computable real. The binary expansion of $\Omega^{(s)}$ has effective dimension $s$. $\Omega^{(s)}$ computes a fixed-point-free real and is of c.e. degree, so by the Arslanov completeness criterion it is Turing complete. Hence it is Turing-equivalent to a 1-random real.

The last questions of this section relate to resource-bounded computation. NP is the class of problems solvable in nondeterministic polynomial time.

**Problem 2.8.** (Lutz.) Is there an oracle relative to which NP has intermediate dimension? I.e., is there an $A$ such that $0 < \dim_{p^A}(NP^A) < 1$?

There are many time- and space-bounded dimension notions; see the 2005 *SIGACT News* survey by Hitchcock, Lutz, and Mayordomo. Kolmogorov complexity characterizations have been found for cdim and $\dim_{\text{pspace}}$, though cdim is the only one with a universal machine. There are also $\dim_p$ (polynomial time) and $\dim_{FS}$ (finite state machines), among others.

**Problem 2.9.** (Mayordomo.) What are the Kolmogorov characterizations of the remaining time- and space-bounded dimension notions? Is there a notion of universal machine?

## 3. $K$-trivial and almost complete reals

### 3.1. Characterizing $K$-trivials.

**Definition 3.1.** The real $X$ is *$K$-trivial* if it has the lowest possible prefix-free complexity: $K(X \upharpoonright n) \leq K(n) + c$ for all $n$.

It is known that noncomputable c.e. $K$-trivial reals exist, and that all are $\Delta^0_2$. In fact, they form an ideal in the $\Delta^0_2$ Turing degrees that is equal to the downward closure of the set of its c.e. members. $K$-triviality is equivalent to the notions *low for 1-random*, *base for 1-randomness*, and *low for $K$*.

The following two questions are about characterizing the $K$-trivials. The first is in terms of supermartingales; the role model is the characterization of the computable sets as exactly those $A$ such that

$$\exists c \forall n [M(A \upharpoonright n) > 2^{n-c}], \tag{3.1}$$

where $M$ is an optimal supermartingale.

**Problem 3.2.** (Stephan, Slaman.) Is there a (super-)martingale characterization of $K$-triviality? In fact, is there any countable set or ideal characterizable in the manner of Equation 3.1 other than the computable sets?

For the $K$-trivials, Stephan has attempted to obtain a bound of the form $> 2^{n-f(n)}$ for some $f$ without success.

Hirschfeldt comments that although $K$-triviality is a robust concept, as shown by the many equivalent characterizations, it does rely on the choice of prefix-free Kolmogorov complexity. There are differences, at the level of $\log n$, between Kolmorogov complexity, martingales, and others. It is possible that studying this question will aid in making fine distinctions between the compressibility and martingale approaches.

*Reverse mathematics* is the program of classifying theorems of ordinary mathematics according to the strength of the set-existence axioms required to prove them. For more on reverse mathematics see Simpson's book *Subsystems of Second-Order Arithmetic*.

**Problem 3.3.** (Hirschfeldt.) Is there a reverse math characterization of the ideal of $K$-trivials? For example, some axiom system such that the intersection of all the $\omega$-models of that system is exactly the $K$-trivials.

3.2. ***K*-trivials and Turing degrees.** The first few problems in this section involve locating the $K$-trivials in the Turing degrees. One positive result is that there is a single Turing-incomplete $\text{low}_2$ degree which is above all c.e. $K$-trivial $A$.

**Problem 3.4.** Is every $K$-trivial $A$ below some incomplete 1-random?

If a set $C$ is computable from both $A$ and $B$, where $A \oplus B$ is random, then $C$ is $K$-trivial.

**Problem 3.5.** Is every $K$-trivial computable from both halves of some random real?

Recall a Turing degree $\boldsymbol{d}$ is *low* if $\boldsymbol{d}' = \emptyset'$. A degree $\boldsymbol{a}$ is *PA* if it is the degree of a complete extension of Peano arithmetic; equivalently, if for all partial computable binary-valued functions $f$, $\boldsymbol{a}$ computes a binary-valued total extension of $f$.

**Problem 3.6.** (Kučera): Is there a single low PA degree that is above every $K$-trivial?

**Update.** Kučera and Slaman have answered this affirmatively; a draft is available at Slaman's webpage.

Nies has shown no single low c.e. degree will work, but that there is a $\text{low}_2$ c.e. degree above all $K$-trivials. It would be equivalent to ask simply if there is a low degree bounding all $K$-trivials, as existence of a low degree implies existence of a low PA degree. Kučera and Slaman have a working version that the answer is yes.

For all $\Delta^0_2$ noncomputable $B$, there is some low $A$ such that $A \oplus B \equiv_T \emptyset'$. $A$ may be chosen 1-generic or PA, but Nies has shown that if $B$ is $K$-trivial, $A$ may not always be chosen 1-random. We may consider the reverse direction.

**Problem 3.7.** (Kučera.) For which $A$ is there a $K$-trivial $B$ such that $A \oplus B$ is complete?

The rest of the degree-theoretic problems in this section involve *almost completeness*, a kind of co-triviality.

**Definition 3.8.** $B$ is *almost complete* (or $\emptyset'$*-trivializing*) if $\emptyset'$ is $K$-trivial relative to $B$.

An almost complete c.e. $B <_T \emptyset'$ may be constructed using Jockusch-Shore pseudojump inversion (Nies), but the construction is indirect and inflexible.

**Problem 3.9.** (Nies.) Is it possible to construct almost complete reals strictly below $\emptyset'$ with upper cone avoidance (i.e., not above $A$ for some given noncomputable c.e. $A$)? Is there a minimal pair of (c.e.) almost complete degrees?

Regarding the latter, it is known there is a minimal pair of c.e. sets such that $\emptyset'$ is $tt$-below the jump of each of them (Shore, unpublished). One may also ask the following:

**Problem 3.10.** Is there a minimal pair of (u.)a.e. dominating degrees?

A Turing degree $\boldsymbol{a}$ is *almost everywhere dominating* (a.e. dominating) if for almost all $X \in 2^\omega$ (with respect to the standard measure) and for all $g : \omega \to \omega$ such that $g \leq_T X$, there is a function $f : \omega \to \omega$ of degree $\boldsymbol{a}$ which dominates $g$ (i.e., on some infinite tail of the natural numbers $f(n) > g(n)$). The degree $\boldsymbol{a}$ is *uniformly almost everywhere dominating* (u.a.e. dominating) if a single $f$ works

for almost every $X$ and all $g$ computable from those $X$. These two domination properties are equivalent.

In the $\Delta^0_2$ degrees, (u.)a.e. domination is equivalent to almost completeness, but in general domination is weaker, so 3.10 is a distinct question from part two of 3.9.

**Problem 3.11.** (Nies.) Is there a $K$-trivial c.e. set $A$ and an almost complete 1-random $Z$ such that $A \not\leq_T Z$?

**Problem 3.12.** Is every $K$-trivial Turing reducible to every $\Delta^0_2$ almost-complete real?

For any incomplete $\Delta^0_2$ $B$ there is an almost complete PA $A$ which joins with $B$ to $\emptyset'$. This theorem fails if PA is replaced by 1-random.

**Problem 3.13.** (Kučera.) What is the connection between almost complete PA and almost complete 1-random? That is, which almost complete PA degrees bound almost complete 1-randoms, if any do? Given an almost complete 1-random, is there an almost complete PA degree in the interval between the random and $\emptyset'$?

Kučera and Slaman have some results in this direction.

**Problem 3.14.** (Nies.) For a time bound $g$, say a polynomial, let $K^g(x)$ be the minimum length of a description $\sigma$ such that the universal machine produces $x$ from input $\sigma$ in no more than $g(|x|)$ steps. Study $K^g$-triviality.

## 4. Computational power, halting probabilities, and relative randomness

**Problem 4.1.** Thinking of a random sequence as the characteristic function of a set, does every infinite subset of that set compute a random? Is there *some* random sequence for which this is true?

The conjecture is no, but a positive result even for the restricted version might have reverse mathematics content, such as showing the axiom system $\mathrm{SRT}^2_2$ (stable Ramsey's theorem for pairs and 2 colors) implies $\mathrm{WWKL}_0$ (weak weak König's lemma).

Call $X$ *complex* (or a *complex real*) if $K(X \upharpoonright n) \geq h(n)$ for some computable, unbounded, nondecreasing function $h$. It is known such reals exist, and known not every complex real computes a random real. This is for unspecified $h$, however. What happens when we look at specific $h$?

**Problem 4.2.** (Hirschfeldt, Reimann.) Is there a (computable,) unbounded function $h$ such that $K(X \upharpoonright n) \geq n - h(n)$ implies $X$ computes some 1-random real?

Likewise we can consider possible relationships between lower bounds.

**Problem 4.3.** (Reimann.) Suppose $K(Y \upharpoonright n) \geq g(n)$ for some appropriate $g$, and $X \leq_T Y$. How large can $h$ be in the inequality $K(X \upharpoonright n) \geq h(x)$?

We could also ask about particular functions $h$. For example, if $X$ is such that $K(X \upharpoonright n) \geq n - \log\log n$, what can be said about $X$ in terms of computational power?

We say a real $X$ is $A$-random, or random relative to $A$, if $X$ passes all $A$-Martin-Löf tests: tests where the sets are uniformly $\Sigma^A_1$.

**Problem 4.4.** (Downey, Stephan.) Define the set $\mathrm{Rand}_B^A$ by

$$\mathrm{Rand}_B^A = \{X : X \text{ is } A\text{-random and } X, B \text{ are a minimal pair in the T-degrees}\}.$$

For which pairs $A, B$ does $\mathrm{Rand}_B^A$ satisfy the following generalization of van Lambalgen's theorem?

**Theorem.** For all $X, Y$, the following are equivalent:

(i) $X \oplus Y \in \mathrm{Rand}_B^A$
(ii) $X \in \mathrm{Rand}_B^A$ and $Y \in \mathrm{Rand}_{B\oplus X}^{A\oplus X}$
(iii) $Y \in \mathrm{Rand}_B^A$ and $X \in \mathrm{Rand}_{B\oplus Y}^{A\oplus Y}$

The motivation behind this problem is that when $B$ is $\emptyset'$ and $A$ is $\emptyset$, $\mathrm{Rand}_B^A$ is the set of weakly 2-random reals.

**Definition 4.5.** An $\Omega$-*number* is a real that is 1-random and left-c.e.; each is the halting probability of *some* universal prefix-free Turing machine.

$A$ is *strong weak truth table reducible* (sw-reducible) to $B$, $A \leq_{sw} B$, if there is a functional $\Gamma$ such that $\Gamma^B = A$ and the use of $\Gamma^B(n)$ is bounded by $n + \mathcal{O}(1)$.

**Problem 4.6.** Are there $\Omega$-numbers $\Omega_0$ and $\Omega_1$ such that one is strictly tt-below the other? sw-below? It is known that a tt-incomparable pair exist.

Let the probability of a universal machine $U$ halting with output in some set $X \subseteq 2^{<\omega}$ be

$$\Omega_U[X] = \sum_{\substack{p \in \mathrm{dom}(U) \\ U(p) \in X}} 2^{-|p|}.$$

It is known that if $X$ is c.e. and infinite, $\Omega_U[X]$ is an $\Omega$-number (in particular, random), but if $X$ is allowed to be $\Delta_2^0$, $\Omega_U[X]$ can be rational – in fact, for any universal machine $U$ and $n \in \omega$, there is some $X \leq_T \emptyset'$ such that $\Omega_U[X] = \frac{1}{n}$.

**Problem 4.7.** (Becher, Figueira, Grigorieff, Miller.) What are the possible values of $\Omega_U[X]$ for, say, co-c.e. $X$?

Figueira, Stephan, and Wu have constructed a *particular* universal machine $U$ and co-c.e. $X$ such that $\Omega_U[X]$ is nonrandom. One improvement gives that for all sufficiently small $K$-trivial numbers $R$ there is a co-c.e. set $X$ with $\Omega_U[X] = R$ for this $U$. What happens with arbitrary universal machines is open, however.

The particular $U$ constructed by Figueira, Stephan, and Wu is not made universal by adjunction (coding all Turing machines into it), it is universal by virtue of generating $K(x)$ up to a constant for all $x$. Any Turing machine $U$ which is universal by adjunction has the property that $\Omega_U[\{x\}]$ is ML-random.

A different approach to halting probabilities gives the following result.

**Theorem 4.8** (Becher/Grigorieff)**.** *Let $A \subset \mathcal{P}(\mathbb{N})$, and let $U : 2^\omega \to \mathcal{P}(\mathbb{N})$ be universal, effective, and continuous. If $U^{-1}(A)$ is $\Sigma_n^0(2^\omega)$ and $A$ is effectively Wadge hard with respect to the class $\Sigma_n^0(2^\omega)$, then $\Omega[A]$ is $n$-random.*

Here "universal" means the function can simulate any other function, effective and continuous means $U(\alpha) = \lim_{n\to\infty} f(\alpha \upharpoonright n)$ for $f$ a recursive function from finite strings to finite subsets of $\mathbb{N}$, and $\Omega[A] = \mu(U^{-1}(A))$ where $\mu$ is Lebesgue measure. Note this is distinct from the previous definitions of $\Omega$; here we must consider infinite computations because $A$ is a subset of $\mathcal{P}(\mathbb{N})$.

$A$ is *effectively Wadge hard with respect to* $\mathcal{C}$ if and only if $\forall B \in \mathcal{C}\ \exists F : \mathcal{C} \to \mathcal{P}(\mathbb{N})$ such that $F$ is effectively continuous and $F^{-1}(A) = B$.

The distinction between $2^\omega$ and $\mathcal{P}(\mathbb{N})$ is topological; $\mathcal{P}(\mathbb{N})$ may be replaced with more general spaces. The topology on $\mathcal{P}(\mathbb{N})$ is the upper cone or spectral topology, generated by all $\mathcal{B}_A = \{B \in \mathcal{P}(\mathbb{N}) : B \supseteq A\}$ where $A$ is finite.

**Problem 4.9.** (Becher.) Does the converse to Theorem 4.8 hold?

The conjecture is yes, though it may be required that "$\Omega[A]$ is $n$-left-c.e." be explicitly added to the conclusion of the theorem. It is open even for $n = 1$. A subsidiary question is to find some $A$ such that the hypothesis of the theorem holds; any $A$ containing the cofinite sets will do.

The theorem also holds if effectively Wadge hard is replaced by *measure Wadge hard*, where $F^{-1}(A) = B$ in the definition of effectively Wadge hard is relaxed to $\mu(F^{-1}(A)) = \mu(B)$.

**Problem 4.10.** Does the (weaker) converse of this theorem hold even if the converse of the original theorem does not?

## 5. Reducibilities

To compare the initial segment complexity of different reals, we define *$K$-reduction*: $A \leq_K B$ means $K(A \upharpoonright n) \leq K(B \upharpoonright n) + c$. *$C$-reduction* is defined in the same way, with plain complexity in place of $K$. A slightly different approach gives *relative $K$-reduction*: $A \leq_{rK} B$ means $(\exists c) K(A \upharpoonright n | B \upharpoonright n) \leq c$.

We know every real is computable from a 1-random real (Kučera-Gács), and that this is in fact a wtt-reduction with low use (Gács), but not just use $= n$. Hence the following remains open.

**Problem 5.1.** Is every real $K$-reducible to a 1-random? $C$-reducible? $rK$-reducible?

The last question can be seen as a nonuniform version of the same question for $\leq_{sw}$ (where Hirschfeldt has shown it fails) by thinking of it as a wtt reduction with bound $n$, plus finitely-much advice (the constant $c$).

**Definition 5.2.** $B$ is *low for random relative to* $A$, $B \leq_{LR} A$, if all $Z$ that are $A$-random are also $B$-random.

**Problem 5.3.** (Nies.) Are the c.e. LR-degrees dense? What other properties do they have, in comparison to the c.e. Turing degrees?

The first question below is a version of the "hungry sets" theorem that shows every base for 1-randomness is $K$-trivial; this has $\leq_{LR}$ in place of $\leq T$.

**Problem 5.4.** (Simpson.) If $A \leq_{LR} B$ and $B$ is random relative to $A$, does it follow that $B$ must be $K$-trivial? Alternatively, if $A \oplus B \leq_{LR} B$ (meaning $A$ is $K$-trivial in $B$) and $B$ is $A$-random, is $A$ necessarily $K$-trivial? Is it possible conversely to characterize LR-reduction in terms of relative $K$-triviality?

**Problem 5.5.** If $A$ is random, $A \leq_{LR} B$, and $B$ is $C$-random, does this imply that $A$ is $C$-random?

## 6. Other kinds of randomness

The major open problem in this area is:

**Problem 6.1.** Is Kolmogorov-Loveland randomness equivalent to Martin-Löf randomness?

ML-random reals defeat all c.e. monotonic betting strategies; KL-random reals defeat all computable nonmonotonic betting strategies. The next position bet on by a nonmonotonic strategy is determined by the results of bets placed thus far. It is important to note these nonmonotonic strategies may be partial; if they are required to be total they have no more power than computable monotonic strategies. The partiality may be in either of two senses: the martingale is not required to converge on all reals, or it is not required to consider all positions of reals on which it does converge. Either sense of partiality is sufficient.

It is known that KL-randomness is strictly stronger than computable randomness (defeating all computable martingales), and implied by 1-randomness. It is also known that no nonmonotonic partial computable strategy can succeed on all c.e. sets, because a set may be enumerated specifically to fail. However, there are pairs of such strategies such that the union of their success sets contains all c.e. sets.

Easier versions of this question may be found in Miller-Nies. For example, a *permutation random* real defeats nonmonotonic martingales for which the order of the positions to be checked is specified in advance. This seems a much weaker concept of randomness, and yet it has not been separated from Martin-Löf randomness.

**Problem 6.2.** Is permutation randomness equivalent to ML-randomness?

**Update.** Kastermans and Lempp have announced a negative answer to this question, presented by Kastermans at the Sept 2007 Chicago workshop.

**Problem 6.3.** Is ML-randomness equivalent to KL-randomness on the left-c.e. reals?

*Kolmogorov-Loveland stochasticity* also uses nonmonotonicity, but instead of betting on the value of the bit in a given location, we choose whether to include it in a subsequence or not. To be KL-stochastic, then, is to have the property that every infinite subsequence selected by a computable rule has limiting frequency of 1s equal to $\frac{1}{2}$. Shen proved KL-stochasticity does not imply ML-randomness, and that ML-random implies KL-stochastic is clear.

**Problem 6.4.** (Reimann.) Find an explicit construction of a KL-stochastic sequence.

**Problem 6.5.** Let $\mathcal{RC}$ be the set of strings which are random with respect to plain complexity: $\{\sigma : C(\sigma) \geq |\sigma|\}$. Is $\emptyset'$ tt-reducible to $\mathcal{RC}$ in polynomial time?

The conjecture is no, that there should even be computable sets that are not poly-time tt-reducible to $\mathcal{RC}$, although without the stipulation of polynomial time, the answer is yes (Kummer). The tt-reduction is not an obvious one, though, and this question could in fact depend on the particular representative of $\emptyset'$ chosen.

Recall *computable randomness* is the notion that no computable martingale succeeds on $X$; it is strictly weaker than 1-randomness. *Schnorr randomness* is randomness relative to the set of Martin-Löf tests where the measure of the $n^{th}$ set is exactly $2^{-n}$ rather than just bounded by $2^{-n}$. It is strictly weaker than computable randomness. The first of the following questions is prerequisite to the second.

**Problem 6.6.** (Franklin.) Is there a machine characterization of computable randomness (i.e., in terms of computational complexity)? Is there a notion of triviality for computable randomness?

The set $A$ is a *base* for a notion $\mathcal{R}$ of randomness if there is some $B \geq_T A$ such that $B$ is $\mathcal{R}$-random relative to $A$.

**Problem 6.7.** What are the bases for Schnorr randomness? Computable randomness?

For computable randomness, the set of bases includes all non-DNC $\Delta^0_2$ sets, and does not include any set of PA degree (Hirschfeldt, Nies, Stephan: "Using random sets as oracles"). As a corollary this shows among the $n$-c.e. sets, the bases for computable randomness are exactly the Turing incomplete sets. Any base for computable randomness is a base for Schnorr randomness, so Schnorr bases exist.

Let the set $\mathrm{NCR}_n$ consist of all reals $X$ such that there is no continuous measure with respect to which $X$ is $n$-random. No characterization is known for $\mathrm{NCR}_n$ for any $n$. For $n = 1$, it is known that $\mathrm{NCR}_1 \subset \Delta^1_1$. Also, if $P$ is a countable $\Pi^0_1$ class, $P \subseteq \mathrm{NCR}_1$ (Kjos-Hanssen, Montalban).

**Problem 6.8.** (Reimann, Slaman.) Does membership in countable $\Pi^0_1$ classes characterize the elements of $\mathrm{NCR}_1$?

**Problem 6.9.** Investigate the analogues to $\mathrm{NCR}_n$ when the measure is allowed to be discontinuous, perhaps with restrictions placing it between "continuous" and "arbitrary".

Finally, a semi-philosophical question. The fact that reals like Chaitin's $\Omega$ are 1-random make a case for saying 1-randomness is not strong enough to give truly random behavior. This problem disappears at the level of 2-randomness, and possibly even just at weak 2-randomness. In fact, recent results by Stephan indicate a large divide between 1-randoms Turing above $\emptyset'$ and not, perhaps allowing us to rescue a subset of 1-randomness as the level of true randomness.

**Problem 6.10.** (Hirschfeldt.) Provide more evidence (mathematical or foundational) for distinguishing some level of randomness as the one at which "truly random" behavior begins.

## 7. Trees and functions

### 7.1. **Mass problems and randomness.**

**Definition 7.1.** A $\Pi^0_1$ *class* is the collection of infinite paths through some subtree of $2^{<\omega}$ that is computable as a set of finite strings.

A *mass problem* is simply a collection of sets, often a $\Pi^0_1$ class. If $P$ and $Q$ are mass problems, $P$ is *weakly reducible* (or Muchnik reducible) to $Q$ if every member of $Q$ Turing computes a member of $P$ by some Turing functional. $P$ is *strongly* (or Medvedev) *reducible* to $Q$ if every member of $Q$ computes a member of $P$ via the same Turing functional. Each notion induces a degree structure of equivalence classes. The countable distributive lattice $\mathcal{P}_w$ is the lattice of weak degrees of mass problems given by nonempty $\Pi^0_1$ classes.

Several examples of intermediate degrees in $\mathcal{P}_w$ are obtained from randomness. The degree of the infimum of the class of 2-randoms and $\emptyset'$, $\inf(r_2, \emptyset')$, is also the maximum weak degree of $\Pi^0_1$ classes with Turing upward closure of positive measure. The degree of the class of 1-randoms, $r_1$ is also the maximum weak degree of $\Pi^0_1$ sets which themselves have positive measure.

**Problem 7.2.** (Simpson.) Are more examples obtainable by replacing measure with classical Hausdorff dimension or constructive dimension? For example, among all weak degrees of (Turing upward closures of) $\Pi^0_1$ classes of positive dimension, is there a largest?

If more weak degree examples may be obtained, what are the relationships among them and between them and previously-known examples?

**Problem 7.3.** (Simpson.) Define $P_s$ as $\{X : \dim(X) = s\}$, or with $> s$ or $\geq s$. The weak degree of $P_s$ is in $\mathcal{P}_w$. Are these degrees the same as random? If not, what are they?

A $\Pi^0_1$ class $P$ is *thin* if every $\Pi^0_1$ subclass of $P$ is relatively clopen; that is, there is some $Q$ that is both closed and open so that the subclass is $P \cap Q$. $P$ is *perfect* if it has no isolated paths; that is, every node is extended by a branching node. Perfect thin $\Pi^0_1$ classes have measure 0, and Binns has shown they have classical Hausdorff dimension 0.

**Problem 7.4.** (Simpson.) Do perfect thin $\Pi^0_1$ classes have effective dimension 0?

After the workshop Binns answered this question in the affirmative.

7.2. **Random closed sets.** By *closed set* we mean a subtree of $2^\omega$, not restricting to $\Pi^0_1$ classes. Cenzer defined a coding on closed sets as follows: the code will be an element of $3^\omega$. The bits correspond to the nodes of the tree in lexicographical order, omitting those which are not part of any path of the closed set. The bit corresponding to node $\sigma$ in the code is 0 or 1 if only $\sigma 0$ or $\sigma 1$, respectively, is in the tree. It is 2 if both $\sigma 0, \sigma 1$ are in the tree. Randomness is then defined just as with Martin-Löf, with a "three-headed coin" probability measure: each of 0, 1, 2 has probability $\frac{1}{3}$.

It is known that a random closed set can contain no computable member, and that it may contain a $\Delta^0_2$ member.

**Problem 7.5.** (Cenzer, Kjos-Hanssen.) Can a random closed set have a c.e. member? d.c.e.? $n$-c.e.?

**Update.** Barmpalias, Brodhead, Cenzer, Dashti, and Weber have shown no random closed set can have an $f$-c.e. member for any computable $f$ bounded by a polynomial. (Algorithmic randomness of closed sets, *Journal for Logic and Computation*, to appear.)

**Problem 7.6.** What is the Medvedev or Muchnik degree of a random closed set?

**Problem 7.7.** If $Q \subseteq 2^\omega$ is a random closed set, what is the effective Hausdorff dimension of $Q$? Of its paths? Are they greater than 0?

7.3. **Random continuous functions.** A continuous function $F : 2^\omega \to 2^\omega$ (i.e., one with a closed graph) may be represented by a function $f : 2^{<\omega} \to 2^{<\omega}$ such that for all $\sigma \in 2^{<\omega}$,

(i) $|f(\sigma)| \leq |\sigma|$, $f(\sigma^\frown i) \leq f(\sigma) + 1$,
(ii) $\sigma_1 \subset \sigma_2 \Rightarrow f(\sigma_1) \subset f(\sigma_2)$,
(iii) for every $n$ there is $m$ such that for all $\sigma$ of length $m$, $|f(\sigma)| \geq n$, and
(iv) for all $X \in 2^\omega$, $F(X) = \bigcup_n f(X \upharpoonright n)$.

Note that a single function $F$ will have many representations $f$, because additional 2s slow the convergence of the image but leave the function unchanged. The canonical representation is that for which the most information available at any given length is used, while preserving the conditions above. Therefore a canonical representing function $f$ would not be able to have, e.g., $f(\sigma) = f(\sigma^\frown 1)$ only to have $f(\sigma^\frown 10) = f(\sigma^\frown 11) = f(\sigma^\frown 1)^\frown 1$. The 1 would be required at the $f(\sigma^\frown 1)$ level.

Once this $f$ is defined, we code it similarly to a closed set. For the bit representing $\sigma^\frown i$, the three outcomes here are 2: $f(\sigma^\frown i) = f(\sigma)$; 1, 0: $f(\sigma^\frown i) = f(\sigma)^\frown 1$ or $f(\sigma)^\frown 0$. Each is assigned probability $\frac{1}{3}$ and randomness is defined à la Martin-Löf.

Kjos-Hanssen sketched a proof that the value of a random continuous function at a computable point will be random, which has since been developed into a full proof. He claimed that an analogous result would hold for Asarin-Pokrovskiy random Brownian motions, discussed below.

**Problem 7.8.** (Becher.) When is the composition of two continuous random functions random?

**Problem 7.9.** (Becher.) Is there a notion of triviality? If so, what happens when a random function is composed with a trivial one?

**Problem 7.10.** (Becher.) What geometric operations can be devised that preserve randomness?

Cenzer's notion of random continuous function differs from Brownian motion, in that he considers functions only from $[0, 1]$ to $[0, 1]$, whereas Brownian motion on $[0, 1]$ will with positive probability move outside of any compact interval. The literature provides two equivalent notions of randomness for Brownian motion, one due to Asarin and Pokrovskiy, 1986, and one to Fouché, 2000. For definitions and proof of their equivalence one can consult the 1986 paper in *Automation and Remote Control* **47**, 21–28.

**Problem 7.11.** The Asarin-Pokrovskiy definitions codes functions non-uniquely. Are all codes for a given function of the same or similar Kolmogorov complexity? Could a random function have a $K$-trivial representation?

**Problem 7.12.** (Becher.) Is there some specific example of a random Brownian motion?

## 8. Computation and information theory

The problem of computation in the presence of random noise may be solved by replacing every bit of the tape of a Turing machine by a finite automaton, where corresponding cells of the automata perform independent Turing computation steps, and then each automaton performs an error-correcting step. The consensus among varying cell-tracks will be the correct answer with probability 1. However, this is usually paid for by a blowup in computation time and space. Gács produced an

efficient, reliable machine using one-dimensional automata, but it is highly complicated and difficult to understand. Levin (et al) produced a one-dimensional automaton which appears to correct for symmetric constant noise under 20%, but it has not been proven to do so. Asymmetric noise, however, will certainly destroy the information.

**Problem 8.1.** (Levin.) Find a simple automaton which, like Gács', can maintain its information despite even asymmetric noise.

*Mutual information* for finite strings $x, y$ is defined as

$$I(x : y) = K(x) + K(y) - K(x, y) = \log \frac{m(x, y)}{m(x)m(y)},$$

where $m$ is the universal probability measure. There are several proposed definitions for mutual information for infinite strings. For example, a straightforward analogue of the finite definition would be

$$I(\alpha : \beta) = \log \sum_{x,y} m(x|\alpha)m(y|\beta)\frac{m(x, y)}{m(x)m(y)}. \tag{8.1}$$

As an aside, it may be that we can restrict to $x = y$ in (8.1). If allowing $x \neq y$ is not necessary the definition would be simplified quite a bit.

**Problem 8.2.** (Levin.) Taking the definition of mutual information as (8.1), is it the case that $I(A : A) < \infty$ implies $A$ is $K$-trivial?

The converse is true, because $A$ $K$-trivial implies $m(x|A) \approx m(x)$, so what remains is $\log \sum_{x,y} m(x, y)$, which converges. This question relates to the following:

**Problem 8.3.** (Levin.) Which definition of mutual information for infinite strings is the "right" one?

We may look for correspondence to other "natural" properties; for instance, we may require that finite mutual information with oneself under that definition of $I$ implies $K$-triviality. $I(A : B) < \infty$ implying $A, B$ form a minimal pair in the LR or LK degrees would also be good evidence that $I$ is the right $I$.