Measuring the Randomness of Random Reals

Joseph S. Miller

VIC2004

Wellington, New Zealand

February 12, 2004

Question: When is one real (element of 2^ω) *more random* than another?

Clear if one is random and the other not, but what if:

1. Both are non-random?
2. Both are random?

In this talk we are primarily interested in the second case.

Quick review

$\mathcal{U}^Z\colon 2^{<\omega} \to 2^{<\omega}$ is a universal prefix-free machine with oracle $Z \in 2^\omega$.

- *prefix-free* $\equiv$ if $x, y \in \text{domain}(\mathcal{U}^Z)$ then $x \not\prec y$.
- *universal* $\equiv$ simulates any other such machine.

Def (Prefix-free complexity).
$K^Z(x) = \min\{|y| \mid \mathcal{U}^Z(y) = x\}$.

- Well defined (for each Z) up to a constant.
- $K(x) \equiv K^\emptyset(x)$.

. . . review continued

Def (Chaitin). A is 1-Z-random if $(\forall n) K^Z(A \upharpoonright n) \geq n + \mathcal{O}(1)$.

i.e., random strings are *incompressible.*

- 1-random $\equiv$ 1-$\emptyset$-random.
- n-random $\equiv$ 1-$\emptyset^{(n-1)}$-random.

Same as Martin-Löf random.

Degrees of randomness: history

- (Solovay) introduced $\leq_S$ and, implicitly, $\leq_K$ and $\leq_C$.
- (Downey, Hirschfeldt and Laforte) introduced $\leq_{sw}$ and $\leq_{rK}$.

$$
\begin{array}{ccccc}
\leq_S & & & & \leq_K \\
 & \searrow & & \nearrow & \\
\not\updownarrow & & \leq_{rK} & & \not\downarrow \uparrow ? \\
 & \nearrow & & \searrow & \\
\leq_{sw} & & & & \leq_C
\end{array}
$$

. . . history continued

Most initial work done for c.e. reals where the degree structures are nice.

- c.e. real $\equiv$ limit of increasing computable sequence.

Thm (Downey, Hirschfedlt, Nies, Laforte). On the c.e. reals, $\leq_S$, $\leq_{rK}$, $\leq_K$ and $\leq_C$ all induce dense uppersemilattices. The top degree is the random c.e. reals and $+$ is the join.

For general reals, the structures are less well-behaved and less understood.

Question: Do these reducibilities help us compare the degree of randomness of random reals?

$\leq_{rK}$ is way too strong:

Thm. The $\leq_{rK}$ degrees of 1-randoms form an antichain.

It is *unknown* if this theorem is true of $\leq_K$ (or $\leq_C$).

Def. $A \leq_K B$ if
$(\forall n) K(A \upharpoonright n) \leq K(B \upharpoonright n) + \mathcal{O}(1)$.

Similarly for $\leq_C$.

K-reducibility is:

- too strong, and
- very hard to work with.

To address both of these concerns we consider two “new” degree structures.

The van Lambalgen Degrees

Def. $A \leq_{vL} B$ if $(\forall C) A \oplus C$ is 1-random $\implies$ $B \oplus C$ is 1-random.

Inspired by:

Thm (van Lambalgen). $A \oplus B$ is 1-random iff A is 1-random and B is 1-A-random.

Actually, $\leq_{vL}$ is not new. It agrees with Nies' $\geq_{LR}$ on the 1-random reals.

Many things are easy to prove for $\leq_{vL}$.

Thm (with Yu Liang).

1. $\mathbf{0}_{vL} = \{A \mid A \text{ not random}\}$.
2. If $A \geq_T B$ and B is 1-random, then $A \leq_{vL} B$.
3. If $A \leq_{vL} B$ and A is n-random, then B is n-random.
4. If $A \oplus B$ is 1-random, then A and B have no vL-upper bound (no join!)
5. If $A \oplus B$ is 1-random, then $A \oplus B <_{vL} A$.
6. No maximal or minimal random vL-degrees.
7. There are 1-random reals $A \equiv_{vL} B$ but $A \not\equiv_T B$.

Note the reversal in 2.

In fact, parts 2 and 3 give:

Thm. A 1-random real computable from an n-random is n-random.

Bounding computational complexity *from above* implies greater randomness (another measure of complexity)!

Heuristic: More random reals are less useful as oracles.

Relating $\leq_K$ to $\leq_{vL}$

With Yu Liang.

Take strings (of length n) to represent natural numbers (between $2^n - 1$ and $2^{n+1} - 2$).

Lemma. $A \oplus C$ is 1-random iff $(\forall n) K(A \upharpoonright (C \upharpoonright n)) \geq C \upharpoonright n + n + \mathcal{O}(1)$.

Thm. $A \leq_K B \implies A \leq_{vL} B$.

Cor.

- If $A \leq_K B$ is and A is n-random, then B is n-random.
- If $A \oplus B$ is 1-random, then A and B have no K-upper bound.

Another degree structure

Def (André Nies). $A \leq_{LK} B$ if $(\forall x) K^A(x) \geq K^B(x) + \mathcal{O}(1)$.

In other words, A is *less useful* than B as an oracle for K.

…or A is closer to being *low for K* (see André's lecture tomorrow).

Thm (André Nies).
$A \equiv_{LK} B \implies A' \equiv_{tt} B'$.

Relating $\leq_K$ to $\geq_{LK}$

Easy fact: $\geq_{LK} \Longrightarrow \leq_{vL}$.

So how do $\leq_K$ and $\geq_{LK}$ relate?

Lemma. If A is 1-random, then $(\forall x)$ $\min_{n \in \mathbb{N}}\{K(A \upharpoonright \langle x, n\rangle) - \langle x, n\rangle\} = K^A(x) + \mathcal{O}(1)$.

Thm. If A is 1-random, then $A \leq_K B$ implies $A \geq_{LK} B$.

Cor. If A is 1-random, then $A \equiv_K B$ implies $A' \equiv_{tt} B'$.

Hence, the K-degree of a 1-random is countable.

By a different (more direct) method:

Thm. If A is 3-random and $A \leq_K B$, then $A' \geq_{tt} B'$.

So, 3-random K-degrees have only countable much above them.

Again, note the reversal between degree of randomness and computational complexity.

Note: It is open if *any* (or *all*) 1-random K-degrees are maximal.

Finally. . .

Thm. If $A \oplus B$ is 1-random, then $A \mid_K A \oplus B$.

But clearly, $A \oplus B \geq_{LK} A$.

Cor. $\geq_{LK}$ does not imply $\leq_K$, even for 1-randoms.

Putting it all together:

$$\leq_K \quad \overset{\not\longleftarrow}{\longrightarrow} \quad \geq_{LK} \quad \longrightarrow \quad \leq_{vL}$$

for 1-randoms.

Thank You.