Excess complexity and degrees of randomness

Joseph S. Miller

Workshop on Computability Theory
Sofia, Bulgaria

August 6, 2009

Kolmogorov complexity

Let $M\colon 2^{<\omega} \to 2^{<\omega}$ be a partial computable function with prefix-free domain (a *machine*).

Definition (Kolmogorov complexity with respect to M)

$$K_M(\sigma) = \min\{|\tau|\colon M(\tau) = \sigma\}.$$

There is a *universal* prefix-free machine U. I.e., one that compresses as well as any other (up to a constant).

Prefix-free (Kolmogorov) complexity

$$K(\sigma) = K_U(\sigma).$$

The complexity of σ is the length of its shortest description.

Initial segment complexity and randomness

For any $A \in 2^\omega$, we have

$$K(n) \leqslant^+ K(A \restriction n) \leqslant^+ n + K(n)$$

Definition

A is 1-*random* if $K(A \restriction n) \geqslant^+ n$.

In other words, random reals are incompressible.

The initial segment complexity of a sequence tells us more than whether it is random. For example:

Theorem

$K(A \restriction n)$ is infinitely often essentially maximal ($n + K(n) + O(1)$) iff A is 2-random (random relative to $\emptyset'$).

1-randoms have excess complexity

A is 1-random…

- iff $K(A \upharpoonright n) \geqslant^+ n$ (Levin; Schnorr)
- iff $K(A \upharpoonright n) - n \to \infty$ (Chaitin)
- iff $\sum_{n \in \omega} 2^{n - K(A \upharpoonright n)} < \infty$ (Ample Excess: M. and Yu).

Any real with initial segment complexity greater than n, has complexity somewhat significantly greater than n.

We will focus on this *excess complexity*.

Gaps

Definition

Let A be 1-random. We call $f\colon \omega \to \omega$ a *gap for* A if:

- f is unbounded,
- f is nondecreasing, and
- $K(A \upharpoonright n) \geqslant^{+} n + f(n)$.

Definition

The *maximal gap for* A is $f(n) = \min_{m \geqslant n} K(A \upharpoonright m) - m$.

We will return to the subject of maximal gaps later.

There is no universal gap

There is no single gap that works for all 1-random reals.

Theorem (Downey and Bienvenu; M. and Yu)

If $f\colon \omega \to \omega$ is *any* unbounded function, then there is a 1-random A such that $(\exists^\infty n)\ K(A \upharpoonright n) < n + f(n)$.

(Downey and Bienvenu proved this under the assumption that f is nondecreasing.)

The proof requires that we exert fairly fine control over dips in $K(A \upharpoonright n) - n$. For that we use *the bounding lemma*.

The bounding lemma

Bounding Lemma (M. and Yu)

If $\sum_{n\in\omega} 2^{-g(n)} < \infty$ and $g \leqslant_T A$ with use n, then $K(A \upharpoonright n) \leqslant^+ n + g(n)$.

Using $g \upharpoonright (n+1)$ we could give every string of length n a description of length $n + g(n) + O(1)$ (Kraft–Chaitin).

Let σ be the description of $A \upharpoonright n$. So σ codes $A \upharpoonright n$, from which we can compute $g \upharpoonright (n+1)$, from which we can decode σ. We would know how to read the message if only we knew what the message said. The heart of the proof is resolving this circularity.

Ample excess is tight

Theorem

If $\sum_{n\in\omega} 2^{-f(n)} < \infty$, then there is a 1-random $A \in 2^\omega$ such that

$$K(A \upharpoonright n) \leqslant^+ n + f(n).$$

Proof Idea.

Find a function g such that

1. $g \leqslant f$,
2. $\sum_{n\in\omega} 2^{-g(n)} < \infty$,
3. g can be coded in a compact way.

Use (Kučera–)Gács to find a 1-random A such that $g \leqslant_T A$ with use n. Apply the bounding lemma. □

There is no universal gap

Theorem (Downey and Bienvenu; M. and Yu)

If $f\colon \omega \to \omega$ is *any* unbounded function, then there is a 1-random A such that $(\exists^\infty n)\ K(A \upharpoonright n) < n + f(n)$.

Proof.

Let g be any function such that

1. $\sum_{n\in\omega} 2^{-g(n)} < \infty$,
2. $\limsup_{n\in\omega} f(n) - g(n) = \infty$.

Apply the previous theorem. □

Review

- Every 1-random admits a gap.
- No gap for all 1-randoms.

Gaps for stronger randomness notions?

An easy extension of the no-gap theorem:

Corollary

If $f\colon \omega \to \omega$ is *any* unbounded function, then there is a weak 2-random A such that $(\exists^\infty n)\ K(A \restriction n) < n + f(n)$.

On the other hand:

Proposition

There is a gap f for every Schnorr 2-random.

We will focus on gaps for 2-random reals.

2-random reals

Solovay first proved the existence of a complexity gap for 2-randomness. He also showed that Ω (Chaitin's halting probability) did not respect this gap. More on Solovay soon…

Recall

Ω is Turing equivalent to $\emptyset'$.

So, A is 2-random…

- iff A is $\emptyset'$-random
- iff A is Ω-random
- iff Ω is A-random (Van Lambalgen's theorem)

A characterization of 2-random reals

Theorem (M. and Yu)

A and B are random relative to each other iff
$$K(A \upharpoonright n) + C(B \upharpoonright n) \geqslant^{+} 2n.$$

Therefore, A is 2-random if and only if

$$K(A \upharpoonright n) \geqslant^{+} n + f(n),$$

where $f(n) = n - C(\Omega \upharpoonright n)$.

This f is *not* nondecreasing, so not a gap. On the other hand, we can show that f is unbounded.

A gap for the 2-random reals

Theorem (Nies, Stephan and Terwijn; M.)

A is 2-random iff $\liminf_{n\to\infty} n - C(A \upharpoonright n) < \infty$.

Since Ω is not 2-random, f is unbounded. Let

$$g(n) = \min_{m \geqslant n} f(m) = \min_{m \geqslant n} m - C(A \upharpoonright m).$$

This is a gap for every 2-random.

Open Question

If g is a gap for A, must A be 2-random?

What's next?

- Characterize 2-randomness with a gap.
- Understand Solovay's work on this subject.

Slow growing functions

Solovay considered two “inverse busy beaver” functions:

$$\begin{aligned} \alpha(n) &= \min_{m \geqslant n} K(m), \\ s(n) &= -\log\left(\sum_{m \geqslant n} 2^{-K(m)}\right). \end{aligned}$$

Both are nondecreasing, unbounded and $\emptyset'$-computable.

Theorem (Solovay)

- $s(n) \leqslant^{+} \alpha(n)$,
- $\alpha(n) \leqslant^{+} s(n) + K(s(n))$.

Solovay's gap for 2-randoms

Theorem (Solovay)

- $K^{\emptyset'}(n) \leqslant K(n) - \alpha(n) + O(\log \alpha(n))$,
- There is a c such that if A is 2-random, then
$$K(A \upharpoonright n) \geqslant n + \alpha(n) - c \log \alpha(n).$$

We show that:

Theorem

- There is no A for which $K(A \upharpoonright n) \geqslant^{+} n + \alpha(n)$,
- A is 2-random if and only if $K(A \upharpoonright n) \geqslant^{+} n + s(n)$.

We have a natural gap characterizing 2-randomness.

Why α is not a gap

Theorem (M. and Yu)

The following are equivalent for g:

1. $\sum_{n\in\omega} 2^{g(n)-K(n,g(n))}$ diverges,
2. For almost every A, it is not the case that $K(A\restriction n) \geqslant^+ n + g(n)$.

Take m such that $\alpha(m) = K(m)$.

Then $K(m, \alpha(m)) = K(m, K(m)) =^+ K(m) = \alpha(m)$, so $2^{\alpha(m)-K(m,\alpha(m))}$ is bounded below for such m. Therefore, $\sum_{n\in\omega} 2^{\alpha(n)-K(n,\alpha(n))}$ diverges.

Therefore, $K(A\restriction n) \not\geqslant^+ n + \alpha(n)$, for almost every A.

Why α is not a gap (cont.)

From:

- $K(A \upharpoonright n) \not\geqslant^+ n + \alpha(n)$, for almost every A, and
- $\alpha \leqslant_T \emptyset'$,

it follows that $K(A \upharpoonright n) \not\geqslant^+ n + \alpha(n)$ when A is 2-random.

But $K(A \upharpoonright n) \geqslant^+ n + \alpha(n)$ implies $K(A \upharpoonright n) \geqslant^+ n + s(n)$ (since $s \leqslant^+ \alpha$), which implies that A is 2-random (see below).

Corollary

There is no A for which $K(A \upharpoonright n) \geqslant^+ n + \alpha(n)$.

A characterization of s

Let $\{\Omega_n\}_{n\in\omega}$ be a computable, non-decreasing sequence of rational numbers converging to Ω.

Definition

$\gamma(n) = -\log(\Omega - \Omega_n)$.

Proposition

The definition of γ is independent, up to a constant, of the choice of Ω and $\{\Omega_n\}_{n\in\omega}$.

This follows from Kučera and Slaman, who show that *every* computable, monotonic sequence approximating a 1-random c.e. real has essentially the same rate of convergence.

A characterization of s (cont.)

$$\begin{aligned} s(n) &= -\log\left(\sum_{m \geqslant n} 2^{-K(m)}\right), \\ \gamma(n) &= -\log(\Omega - \Omega_n). \end{aligned}$$

Proposition

$\gamma(n) =^+ s(n)$.

Proof.

Take $\Omega = \sum_{m \in \omega} 2^{-K(m)}$ and $\Omega_n = \sum_{m < n} 2^{-K_n(m)}$.

Then clearly $\Omega - \Omega_n \geqslant \sum_{m \geqslant n} 2^{-K(m)}$, so $\gamma(n) \leqslant^+ s(n)$.

But $K(m) \leqslant^+ -\log(\Omega_{m+1} - \Omega_m)$, so $s(n) \leqslant^+ \gamma(n)$. □

Another slow growing function

We use another slow growing function and close relative of γ.

Definition

$\widehat{\gamma}(n) = \max\{k\colon \Omega_n \restriction k = \Omega \restriction k\}$.

Notes

- Since $\Omega - \Omega_n \leqslant 2^{-\widehat{\gamma}(n)}$, we have $\widehat{\gamma} \leqslant^+ \gamma$.
- It is not clear that $\widehat{\gamma}$ is independent of the choice of Ω and $\{\Omega_n\}_{n\in\omega}$.
- Also not proved: is $\widehat{\gamma}$ different from γ?

Another gap for 2-random reals

Theorem

The following are equivalent for $A \in 2^\omega$:

1. A is 2-random,
2. $K(A \upharpoonright n) \geqslant^+ n + \gamma(n)$.

The same holds with γ replaced by $\widehat{\gamma}$.

Proof.

We may assume that A is 1-random, otherwise neither condition holds.

(2) $\implies$ (1) for $\widehat{\gamma}$: Define g as follows. To find $g(n)$, look for the the first *unused* $\sigma \in 2^{<\omega}$ such that $U_n^{A \upharpoonright n}(\sigma) = \tau$ and $\Omega_n \upharpoonright |\tau| = \tau$. Mark σ as *used* and set $g(n) = |\sigma|$. Otherwise, let $g(n) = n$.

Proof (cont.)

Note that $g(n)$ can be computed from $A \upharpoonright n$. Also note that $\sum_{n\in\omega} 2^{-g(n)} < \infty$. Therefore, by the bounding lemma, there is a $d \in \omega$ such that $K(A \upharpoonright n) \leqslant n + g(n) + d$.

If Ω is not A-random, fix c and find an m such that $K^A(\Omega \upharpoonright m) \leqslant m - c$. Let σ be a minimal U^A-program for $\Omega \upharpoonright m$. This σ will eventually be used in the definition of g for some n. Thus $g(n) = |\sigma| \leqslant m - c$. But $\Omega_n \upharpoonright m = \Omega \upharpoonright m$, so $\widehat{\gamma}(n) \geqslant m$. Therefore

$$K(A \upharpoonright n) \leqslant n + g(n) + d \leqslant n + m - c + d \leqslant n + \widehat{\gamma}(n) - c + d.$$

For all c, there is such an n, hence $K(A \upharpoonright n) \not\geqslant^+ n + \widehat{\gamma}(n)$.

(1) $\Longrightarrow$ (2) for γ: Use the ample excess lemma. □

Review

Review

- A 1-random implies $K(A \upharpoonright n) - n \to \infty$.
- No lower bound on this divergence works for all weak 2-random reals.
- There is a gap for all Schnorr 2-random reals.
- $\alpha(n) = \min_{m \geqslant n} K(m)$ is not a gap for any 1-random.
- There is a gap $\gamma(n) =^{+} s(n)$ *characterizing* 2-randomness.

Note

It is not the case that $K^{\emptyset'}(n) \leqslant^{+} K(n) - \gamma(n)$.

This is because $\sum_{n \in \omega} 2^{-K(n)+\gamma(n)}$ diverges.

Degrees of randomness

Several partial orders have been proposed to capture the idea that one real is *more random* than another.

Definition (Solovay; Downey, Hirschfeldt and LaForte)

$A \leqslant_K B$ if $K(A \upharpoonright n) \leqslant^+ K(B \upharpoonright n)$.

Definition (M. and Yu)

$A \leqslant_{vL} B$ if $(\forall Z)\ [A \oplus Z$ is 1-random $\implies$ $B \oplus Z$ is 1-random $]$.

Notes

- $A \leqslant_K B \implies A \leqslant_{vL} B$.
- If A and B are 1-random,
$$B \leqslant_T A \implies B \leqslant_{LR} A \iff A \leqslant_{vL} B.$$
- Even vL is very strong; every 1-random is incomparable from almost every real.

A new degree notion

Definition

We write $A \leqslant_g B$ if every gap for A is a gap for B.

Equivalently, the maximal gap for A is a gap for B.

Clearly, $A \leqslant_K B \implies A \leqslant_g B$. We can do better.

Let $\alpha^A(n) = \min_{m \geqslant n} K^A(m)$.

Proposition

If A is 1-random, then $\alpha^A(n) =^+ \min_{m \geqslant n} K(A \upharpoonright m) - m$. In other words, α^A is essentially the maximal gap of A.

Again, one direction follows from the ample excess lemma, the other from the bounding lemma.

A new degree notion (cont.)

Corollary

Let A and B be 1-random. Then $A \leqslant_g B$ iff $\alpha^A(n) \leqslant^+ \alpha^B(n)$.

If A and B are 1-random and $A \leqslant_{vL} B$, then $B \leqslant_{LR} A$, so $K^A(n) \leqslant^+ K^B(n)$ (Kjos-Hanssen, M. and Solomon).

But then $\alpha^A(n) \leqslant^+ \alpha^B(n)$.

Corollary

Let A and B be 1-random. Then $A \leqslant_{vL} B$ implies $A \leqslant_g B$.

What do we know about the *gap* degrees?

Proposition

Ω is below every 2-random.

Proof.

First note that Ω computes γ. But this implies that $\alpha^{\Omega}(n) \leqslant^{+} \gamma$. □

Note that any class *characterized* by a gap is closed upward in the gap degrees. Therefore:

Proposition

If $A \leqslant_g B$ and A is 2-random, then B is 2-random.

It is open whether weak 2-randomness or 3-randomness are closed upward in the gap degrees.

What do we know about the *gap* degrees (cont.)?

Proposition

Every countable set of 1-randoms has a 1-random lower bound in the gap degrees.

Proof.

Let f be a gap for every 1-random in the countable set. Let X be a 1-random computing f (Kučera; Gács). Then $\alpha^X(n) \leqslant^+ f$. □

This is essentially all that is known.

Thank You