Kolmogorov complexity and Solovay functions

Laurent Bienvenu (Ruprecht-Karls Universität Heidelberg, Germany)

(joint work with Rod Downey)

Logic Colloquium
August 1, 2009
Sofia, Bulgaria

Approximating C and K (1)

Plain Kolmogorov complexity C and prefix-free Kolmogorov complexity K are both non-computable functions.

However, they are right-computable i.e. there exists a computable function $(x, s) \mapsto C_s(x)$ such that for all x

- the sequence $s \mapsto C_s(x)$ is nonincreasing
- $\lim_s C_s(x) = C(x)$

and similarly there exists a function $(x, s) \mapsto K_s(x)$ for K.

Approximating C and K (2)

This gives us an easy way to construct computable upper bounds of C or K: take a computable function $t : 2^{<\omega} \to \mathbb{N}$ and set

$$f(x) = C_{t(x)}(x)$$

Then f is a computable upper bound of C.

Approximating C and K (3)

How good are such approximations?

Approximating C and K (3)

How good are such approximations? In general, very bad!!

Proposition

Let f be a computable upper bound of K and Ψ any computable function. There exist infinitely many strings x s.t.

$$f(x) > \Psi(K(x))$$

Upper bounds suffice (1)

Despite this negative result, it turns out that in the theory of randomness for infinite sequences, computable upper bounds of Kolmogorov complexity do a good job.

Upper bounds suffice (1)

Despite this negative result, it turns out that in the theory of randomness for infinite sequences, computable upper bounds of Kolmogorov complexity do a good job.

Let us take for example the celebrated:

Theorem (Levin-Schnorr)

Let $A \in 2^\omega$. Then A is Martin-Löf random if and only if

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

Upper bounds suffice (2)

Theorem (B., Merkle)

Let $A \in 2^\omega$. Then A is Martin-Löf random if and only if for every computable upper bound f of K we have:

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

Upper bounds suffice (2)

Theorem (B., Merkle)

Let $A \in 2^\omega$. Then A is Martin-Löf random if and only if for every computable upper bound f of K we have:

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

Theorem (B., Merkle)

There exists a single computable upper bound F of K such that for all $A \in 2^\omega$, A is Martin-Löf random if and only if

$$F(A \upharpoonright n) \geq n - O(1)$$

Upper bounds suffice (3)

Theorem (Gács / Miller, Yu)

Let $A \in 2^\omega$. Then A is Martin-Löf random if and only if

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

Upper bounds suffice (3)

Theorem (Gács / Miller, Yu)

Let $A \in 2^\omega$. Then A is Martin-Löf random if and only if

$$C(A \restriction n) \geq n - K(n) - O(1)$$

Theorem (Miller, Yu)

Let $A \in 2^\omega$. Then A is Martin-Löf random if and only if for every computable upper bound f of K

$$C(A \restriction n) \geq n - f(n) - O(1)$$

Upper bounds suffice (3)

Theorem (Gács / Miller, Yu)

Let $A \in 2^\omega$. Then A is Martin-Löf random if and only if

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

Theorem (Miller, Yu)

There exists a single computable upper bound F of K such that the following holds. For every $A \in 2^\omega$, A is Martin-Löf random if and only if

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

Approximating well i.o. (1)

We have seen that no computable upper bound of C or K is always accurate. Can we hope for infinitely often accurate?

Approximating well i.o. (1)

We have seen that no computable upper bound of C or K is always accurate. Can we hope for infinitely often accurate?

For C, this is easy. Most strings x satisfy $C(x) = |x| + O(1)$, so take $g(x) = |x| + c$ for an appropriate c, so that $C \leq g$ and $g(x) \leq C(x) + O(1)$ for infinitely many x.

Approximating well i.o. (1)

We have seen that no computable upper bound of C or K is always accurate. Can we hope for infinitely often accurate?

For C, this is easy. Most strings x satisfy $C(x) = |x| + O(1)$, so take $g(x) = |x| + c$ for an appropriate c, so that $C \leq g$ and $g(x) \leq C(x) + O(1)$ for infinitely many x.

What about K? Can we find a computable upper bound g of K such that $g(x) \leq K(x) + O(1)$ for infinitely many x?

Approximating well i.o. (1)

We have seen that no computable upper bound of C or K is always accurate. Can we hope for infinitely often accurate?

For C, this is easy. Most strings x satisfy $C(x) = |x| + O(1)$, so take $g(x) = |x| + c$ for an appropriate c, so that $C \leq g$ and $g(x) \leq C(x) + O(1)$ for infinitely many x.

What about K? Can we find a computable upper bound g of K such that $g(x) \leq K(x) + O(1)$ for infinitely many x?

Harder: a string x has maximal complexity $|x| + K(|x|)$, so it seems that we already need a good approximation of K... a vicious circle!!

Approximating well i.o. (2)

Nonetheless,

Theorem (Solovay)

There exists a computable upper bound g of K such that $g(x) \leq K(x) + O(1)$ for infinitely many x.

Approximating well i.o. (2)

Nonetheless,

Theorem (Solovay)

There exists a computable upper bound g of K such that $g(x) \leq K(x) + O(1)$ for infinitely many x.

Proof.

Given x such that $K(x) = k$, let s be the first integer such that $K_s(x) = k$. Then

$$K\big(\langle x, k, s\rangle\big) = K(x) + O(1)$$

and $\langle x, k, s\rangle$ gives enough information to perform the approximation. □

Solovay functions

Definition

A Solovay function is a computable function f such that

- $K \leq f + O(1)$
- for infinitely many strings x, $f(x) \leq K(x) + O(1)$

A useful criterion

The condition $K \leq f + O(1)$ in the definition is equivalent to $\sum_n 2^{-f(n)} < +\infty$ (identifying $\mathbb{N}$ and $2^{<\omega}$).

A useful criterion

The condition $K \leq f + O(1)$ in the definition is equivalent to $\sum_n 2^{-f(n)} < +\infty$ (identifying $\mathbb{N}$ and $2^{<\omega}$).

Theorem

Let $f : \mathbb{N} \to \mathbb{N}$ be a computable function. Then f is a Solovay function if and only if the sum

$$\sum_n 2^{-f(n)}$$

is finite and is a Martin-Löf random (left-c.e.) real.

A useful criterion (2)

Corollary

If α *and* β *are two left-c.e reals, then* $\alpha + \beta$ *is random if and only either* α *or* β *is random.*

A useful criterion (2)

Corollary

If α and β are two left-c.e reals, then $\alpha + \beta$ is random if and only either α or β is random.

Corollary (Miller)

For any $A \in 2^{\omega}$, the following are equivalent
(i) A is low for Ω (i.e., Ω is A-random)
(ii) A is weakly low for K (i.e., $K(x) = K^A(x) + O(1)$ i.o.)

Solovay functions and randomness

Solovay functions naturally come up in Martin-Löf randomness:

Theorem

Let F be a computable upper bound of K such that for all A

$$A \text{ is Martin-Löf random } \Leftrightarrow F(A \upharpoonright n) \geq n - O(1)$$

Solovay functions and randomness

Solovay functions naturally come up in Martin-Löf randomness:

Theorem

Let F be a computable upper bound of K such that for all A

$$A \text{ is Martin-Löf random } \Leftrightarrow F(A \upharpoonright n) \geq n - O(1)$$

then F must be a Solovay function. (Q: is it sufficient?)

Solovay functions and randomness

Solovay functions naturally come up in Martin-Löf randomness:

Theorem

Let F be a computable upper bound of K such that for all A

$$A \text{ is Martin-Löf random } \Leftrightarrow F(A \upharpoonright n) \geq n - O(1)$$

then F must be a Solovay function. (Q: is it sufficient?)

Theorem

Let F be a computable upper bound of K such that for all A

$$A \text{ is Martin-Löf random } \Leftrightarrow C(A \upharpoonright n) \geq n - F(n) - O(1)$$

then F must be a Solovay function. (Q: is it sufficient?)

Solovay functions and triviality

Recall that A is K-trivial if $K(A \upharpoonright n) \leq K(n) + O(1)$.

Solovay functions and triviality

Recall that A is K-trivial if $K(A \upharpoonright n) \leq K(n) + O(1)$.

Theorem

There exists a single computable upper bound F of K such that for all A:

$$A \text{ is } K\text{-trivial} \Leftrightarrow K(A \upharpoonright n) \leq F(n) + O(1)$$

Solovay functions and triviality

Recall that A is K-trivial if $K(A \upharpoonright n) \leq K(n) + O(1)$.

Theorem

There exists a single computable upper bound F of K such that for all A:

$$A \text{ is } K\text{-trivial} \Leftrightarrow K(A \upharpoonright n) \leq F(n) + O(1)$$

In the proof, F is a Solovay function (the “original” one).

Solovay functions and triviality

Recall that A is K-trivial if $K(A \upharpoonright n) \leq K(n) + O(1)$.

Theorem

There exists a single computable upper bound F of K such that for all A:

$$A \text{ is } K\text{-trivial} \Leftrightarrow K(A \upharpoonright n) \leq F(n) + O(1)$$

In the proof, F is a Solovay function (the “original” one).

But:

- does any Solovay function do the job?
- does F really need to be a Solovay function?

Thank you