

Contrasting plain and prefix-free Kolmogorov complexity

Joseph S. Miller



University of
Connecticut

Kolmogorov Complexity and Applications
Schloß Dagstuhl, Germany

Notation

- C is (plain) Kolmogorov complexity.
- K is prefix(-free Kolmogorov) complexity.

Notation

- C is (plain) Kolmogorov complexity.
- K is prefix(-free Kolmogorov) complexity.
- $KR_c = \{\sigma \in 2^{<\omega} : C(\sigma) \geq |\sigma| - c\}$
(Kolmogorov Random with constant c).

Notation

- C is (plain) Kolmogorov complexity.
- K is prefix(-free Kolmogorov) complexity.
- $KR_c = \{\sigma \in 2^{<\omega} : C(\sigma) \geq |\sigma| - c\}$
(Kolmogorov Random with constant c).
Let $KR = KR_0$.

Notation

- C is (plain) Kolmogorov complexity.
- K is prefix(-free Kolmogorov) complexity.
- $KR_c = \{\sigma \in 2^{<\omega} : C(\sigma) \geq |\sigma| - c\}$
(Kolmogorov Random with constant c).
Let $KR = KR_0$.
- $SCR_c = \{\sigma \in 2^{<\omega} : K(\sigma) \geq |\sigma| + K(|\sigma|) - c\}$
(Strong Chaitin Random with constant c).

- 1 Understand Solovay's [1975] result that Kolmogorov random strings need not be strong Chaitin random (up to a constant).

- 1 Understand Solovay's [1975] result that Kolmogorov random strings need not be strong Chaitin random (up to a constant).
- 2 Understand Muchnik's [2002] result that C and K do not agree *on which strings are more complex* (up to a constant).

- 1 Understand Solovay's [1975] result that Kolmogorov random strings need not be strong Chaitin random (up to a constant).
- 2 Understand Muchnik's [2002] result that C and K do not agree *on which strings are more complex* (up to a constant).
- 3 **Question:** Is SCR_c a Π_1^0 (i.e., co-c.e.) set?

Natural questions

- ① Is K just C pushed up in some monotonic way?

Natural questions

- 1 Is K just C pushed up in some monotonic way?
- 2 Maybe $(\forall \sigma) K(\sigma) = C(\sigma) + K(C(\sigma)) + O(1)$?
(\leq is easy)

Natural questions

- 1 Is K just C pushed up in some monotonic way?
- 2 Maybe $(\forall \sigma) K(\sigma) = C(\sigma) + K(C(\sigma)) + O(1)$?
(\leq is easy)

Both answers are known to be **no**.

Natural questions

- 1 Is K just C pushed up in some monotonic way?
- 2 Maybe $(\forall \sigma) K(\sigma) = C(\sigma) + K(C(\sigma)) + O(1)$?
(\leq is easy)

Both answers are known to be **no**. Solovay (1975) proved that (2) is false; Muchnik (2002) proved that (1) fails.

The Solovay Theorems

Theorem (Solovay, 1975)

For all $\sigma \in 2^{<\omega}$:

- 1 $K(\sigma) = C(\sigma) + C^{(2)}(\sigma) + O(C^{(3)}(\sigma)).$
 $= C(\sigma) + K(C(\sigma)) + O(C^{(3)}(\sigma)).$
- 2 $C(\sigma) = K(\sigma) - K^{(2)}(\sigma) + O(K^{(3)}(\sigma)).$

The Solovay Theorems

Theorem (Solovay, 1975)

For all $\sigma \in 2^{<\omega}$:

- 1 $K(\sigma) = C(\sigma) + C^{(2)}(\sigma) + O(C^{(3)}(\sigma)).$
 $= C(\sigma) + K(C(\sigma)) + O(C^{(3)}(\sigma)).$
- 2 $C(\sigma) = K(\sigma) - K^{(2)}(\sigma) + O(K^{(3)}(\sigma)).$

Theorem (Solovay, 1975)

For some $s \in \omega$, there is a sequence of strings $\{w_m\}_{m \in \omega} \subseteq KR_s$ such that

$$\lim_{m \rightarrow \infty} \frac{|w_m| + K(|w_m|) - K(w_m)}{\log \log |w_m|} = 1.$$

Corollary

The $O(C^{(3)}(\sigma))$ and $O(K^{(3)}(\sigma))$ terms in the Solovay relations are tight.

Corollaries to the second theorem

Corollary

The $O(C^{(3)}(\sigma))$ and $O(K^{(3)}(\sigma))$ terms in the Solovay relations are tight.

Corollary

For some $s \in \omega$ and all $c \in \omega$, $KR_s \not\subseteq SCR_c$.

Corollaries to the second theorem

Corollary

The $O(C^{(3)}(\sigma))$ and $O(K^{(3)}(\sigma))$ terms in the Solovay relations are tight.

Corollary

For some $s \in \omega$ and all $c \in \omega$, $KR_s \not\subseteq SCR_c$.

Note. We will see that $s = 0$ works.

A New Result

Theorem

If $Q \subseteq 2^{<\omega}$ is a Π_1^0 set with strings of every length, then $Q \notin SCR_c$.

A New Result

Theorem

If $Q \subseteq 2^{<\omega}$ is a Π_1^0 set with strings of every length, then $Q \notin SCR_c$.

This answers the open question:

Corollary

For c sufficiently large, SCR_c is not Π_1^0 .

A New Result

Theorem

If $Q \subseteq 2^{<\omega}$ is a Π_1^0 set with strings of every length, then $Q \notin SCR_c$.

This answers the open question:

Corollary

For c sufficiently large, SCR_c is not Π_1^0 .

Proof.

Take c to be large enough to ensure that $(\forall n) SCR_c \cap 2^n \neq \emptyset$.

A New Result

Theorem

If $Q \subseteq 2^{<\omega}$ is a Π_1^0 set with strings of every length, then $Q \notin SCR_c$.

This answers the open question:

Corollary

For c sufficiently large, SCR_c is not Π_1^0 .

Proof.

Take c to be large enough to ensure that $(\forall n) SCR_c \cap 2^n \neq \emptyset$. If SCR_c were Π_1^0 , then the theorem would imply that $SCR_c \notin SCR_c$. \square

Another Consequence

Another Consequence

Corollary (Solovay)

$(\forall c) KR \not\subseteq SCR_c.$

Proof.

KR is Π_1^0 and $(\forall n) KR \cap 2^n \neq \emptyset.$ □

Another Consequence

Corollary (Solovay)

$(\forall c) KR \not\subseteq SCR_c.$

Proof.

KR is Π_1^0 and $(\forall n) KR \cap 2^n \neq \emptyset.$ □

Solovay also proved that $SCR_c \subseteq KR_k$ for sufficiently large k .

Another Consequence

Corollary (Solovay)

$(\forall c) KR \not\subseteq SCR_c.$

Proof.

KR is Π_1^0 and $(\forall n) KR \cap 2^n \neq \emptyset.$ □

Solovay also proved that $SCR_c \subseteq KR_k$ for sufficiently large k .

So having (essentially) maximal K complexity is strictly harder than having (essentially) maximal C complexity.

Muchnik's Theorem

Theorem (An. A. Muchnik, 2002)

For every $d \in \omega$, there are $\sigma, \tau \in 2^{<\omega}$ such that $C(\sigma) - C(\tau) \geq d$ and $K(\tau) - K(\sigma) \geq d$.

Muchnik's Theorem

Theorem (An. A. Muchnik, 2002)

For every $d \in \omega$, there are $\sigma, \tau \in 2^{<\omega}$ such that $C(\sigma) - C(\tau) \geq d$ and $K(\tau) - K(\sigma) \geq d$.

In other words, C and K do not agree (to within any given constant) on which strings are more complex.

Muchnik's Theorem

Theorem (An. A. Muchnik, 2002)

For every $d \in \omega$, there are $\sigma, \tau \in 2^{<\omega}$ such that $C(\sigma) - C(\tau) \geq d$ and $K(\tau) - K(\sigma) \geq d$.

In other words, C and K do not agree (to within any given constant) on which strings are more complex.

This was proved as a corollary to:

Theorem

$\{\langle \sigma, n \rangle \mid K(\sigma) \leq n\}$ may or may not be *tt*-complete, depending on the choice of the universal prefix-free machine U .

Deriving Muchnik's Theorem

Theorem (An. A. Muchnik, 2002)

For every $d \in \omega$, there are $\sigma, \tau \in 2^{<\omega}$ such that $C(\sigma) - C(\tau) \geq d$ and $K(\tau) - K(\sigma) \geq d$.

Proof Sketch.

Fix k such that $(\forall n) SCR_k \cap 2^n \neq \emptyset$.

Deriving Muchnik's Theorem

Theorem (An. A. Muchnik, 2002)

For every $d \in \omega$, there are $\sigma, \tau \in 2^{<\omega}$ such that $C(\sigma) - C(\tau) \geq d$ and $K(\tau) - K(\sigma) \geq d$.

Proof Sketch.

Fix k such that $(\forall n) SCR_k \cap 2^n \neq \emptyset$.

For $c \in \omega$, take $\sigma_c \in KR \setminus SCR_c$. Choose $\tau_c \in SCR_k$ such that $|\tau_c| = |\sigma_c| - \lfloor c/2 \rfloor$.

Deriving Muchnik's Theorem

Theorem (An. A. Muchnik, 2002)

For every $d \in \omega$, there are $\sigma, \tau \in 2^{<\omega}$ such that $C(\sigma) - C(\tau) \geq d$ and $K(\tau) - K(\sigma) \geq d$.

Proof Sketch.

Fix k such that $(\forall n) SCR_k \cap 2^n \neq \emptyset$.

For $c \in \omega$, take $\sigma_c \in KR \setminus SCR_c$. Choose $\tau_c \in SCR_k$ such that $|\tau_c| = |\sigma_c| - \lfloor c/2 \rfloor$. Then $C(\sigma_c) - C(\tau_c) \geq c/2 + O(1)$ and $K(\tau_c) - K(\sigma_c) \geq c/2 - O(\log c)$.

Deriving Muchnik's Theorem

Theorem (An. A. Muchnik, 2002)

For every $d \in \omega$, there are $\sigma, \tau \in 2^{<\omega}$ such that $C(\sigma) - C(\tau) \geq d$ and $K(\tau) - K(\sigma) \geq d$.

Proof Sketch.

Fix k such that $(\forall n) SCR_k \cap 2^n \neq \emptyset$.

For $c \in \omega$, take $\sigma_c \in KR \setminus SCR_c$. Choose $\tau_c \in SCR_k$ such that $|\tau_c| = |\sigma_c| - \lfloor c/2 \rfloor$. Then $C(\sigma_c) - C(\tau_c) \geq c/2 + O(1)$ and $K(\tau_c) - K(\sigma_c) \geq c/2 - O(\log c)$. Therefore, if $c \in \omega$ is sufficiently large, σ_c and τ_c satisfy our requirements. \square

Proving the Basic Theorem

Theorem

If $Q \subseteq 2^{<\omega}$ is a Π_1^0 set such that $(\forall n) Q \cap 2^n \neq \emptyset$, then $Q \notin SCR_c$.

Proving the Basic Theorem

Theorem

If $Q \subseteq 2^{<\omega}$ is a Π_1^0 set such that $(\forall n) Q \cap 2^n \neq \emptyset$, then $Q \notin SCR_c$.

Proof. If $Q \subseteq SCR_c$, then we can force strings to leave Q by ensuring that they are not in SCR_c . *This is the main idea of the proof.*

Proving the Basic Theorem

Theorem

If $Q \subseteq 2^{<\omega}$ is a Π_1^0 set such that $(\forall n) Q \cap 2^n \neq \emptyset$, then $Q \notin SCR_c$.

Proof. If $Q \subseteq SCR_c$, then we can force strings to leave Q by ensuring that they are not in SCR_c . *This is the main idea of the proof.*

We define a prefix-free machine M . By universality, if M gives $\sigma \in 2^{<\omega}$ a description of length c , then $K(\sigma) \leq c + k$ for some k . (By the Recursion Theorem, we can know k .)

Defining M

Defining M

For any stage s and any n such that $K_s(n) < K_{s-1}(n)$, M takes the first $2^{n-k-c-1}$ strings of length n that are still in Q_s and gives these strings descriptions of length

$$n + K_s(n) - k - c - 1.$$

Defining M

For any stage s and any n such that $K_s(n) < K_{s-1}(n)$, M takes the first $2^{n-k-c-1}$ strings of length n that are still in Q_s and gives these strings descriptions of length

$$n + K_s(n) - k - c - 1.$$

If there are not enough strings in $Q_s \cap 2^n$, then M makes due with the available strings.

Defining M

For any stage s and any n such that $K_s(n) < K_{s-1}(n)$, M takes the first $2^{n-k-c-1}$ strings of length n that are still in Q_s and gives these strings descriptions of length

$$n + K_s(n) - k - c - 1.$$

If there are not enough strings in $Q_s \cap 2^n$, then M makes due with the available strings.

It is straightforward to check that M will not run out of room in its domain. (It uses no more of its domain than U does.)

What M does for us

What M does for us

If $|Q_s \cap 2^n| \leq b2^{n-k-c-1}$ for $b > 0$ and $K_{s-1}(n)$ is wrong, then M guarantees that

$$|Q \cap 2^n| \leq (b - 1)2^{n-k-c-1}.$$

What M does for us

If $|Q_s \cap 2^n| \leq b2^{n-k-c-1}$ for $b > 0$ and $K_{s-1}(n)$ is wrong, then M guarantees that

$$|Q \cap 2^n| \leq (b - 1)2^{n-k-c-1}.$$

Why?

What M does for us

If $|Q_s \cap 2^n| \leq b2^{n-k-c-1}$ for $b > 0$ and $K_{s-1}(n)$ is wrong, then M guarantees that

$$|Q \cap 2^n| \leq (b - 1)2^{n-k-c-1}.$$

Why? Let $t \geq s$ be the least stage such that $K_t(n)$ is correct. Then M makes sure that U gives $2^{n-k-c-1}$ strings in $Q_t \cap 2^n$ (if enough are left) descriptions of length $n + K(n) - c - 1$.

Each such string is not in SCR_c (hence not in Q).

Guessing values of $K(n)$

Let b be the least natural number such that

$$(\exists^\infty n) |Q \cap 2^n| \leq b2^{n-k-c-1}.$$

Guessing values of $K(n)$

Let b be the least natural number such that

$$(\exists^\infty n) |Q \cap 2^n| \leq b2^{n-k-c-1}.$$

Note that b cannot be zero, because $(\forall n) |Q \cap 2^n| > 0$.

Guessing values of $K(n)$

Let b be the least natural number such that
$$(\exists^\infty n) |Q \cap 2^n| \leq b2^{n-k-c-1}.$$

Note that b cannot be zero, because $(\forall n) |Q \cap 2^n| > 0$.

Define a partial computable function ψ as follows. If s is the first stage such that $|Q_s \cap 2^n| \leq b2^{n-k-c-1}$, then let $\psi(n) = K_{s-1}(n)$.

Contradiction!

But if $\psi(n)$ is defined and $\psi(n) \neq K(n)$, then
 $|Q \cap 2^n| \leq (b-1)2^{n-k-c-1}$.

Contradiction!

But if $\psi(n)$ is defined and $\psi(n) \neq K(n)$, then $|Q \cap 2^n| \leq (b-1)2^{n-k-c-1}$. Therefore, this can happen only finitely often. Also, the choice of b guarantees that ψ has an infinite domain.

Contradiction!

But if $\psi(n)$ is defined and $\psi(n) \neq K(n)$, then $|Q \cap 2^n| \leq (b-1)2^{n-k-c-1}$. Therefore, this can happen only finitely often. Also, the choice of b guarantees that ψ has an infinite domain.

It is straightforward to derive a contradiction. □

Extending the Basic Result

Theorem

For any $c \in \omega$, $\limsup_{n \rightarrow \infty} \frac{|KR \cap 2^n \setminus SCR_c|}{2^n} > 0$.

Extending the Basic Result

Theorem

For any $c \in \omega$, $\limsup_{n \rightarrow \infty} \frac{|KR \cap 2^n \setminus SCR_c|}{2^n} > 0$.

Which Π_1^0 sets can be subsets of SCR_c ?

Extending the Basic Result

Theorem

For any $c \in \omega$, $\limsup_{n \rightarrow \infty} \frac{|KR \cap 2^n \setminus SCR_c|}{2^n} > 0$.

Which Π_1^0 sets can be subsets of SCR_c ? Partial answer:

Definition

An infinite set $Q \subseteq 2^{<\omega}$ is **not hyperimmune** if there is a computable function $f: \omega \rightarrow \omega$ such that

$$(\forall n) |Q \cap 2^{\leq f(n)}| \geq n.$$

Extending the Basic Result

Theorem

For any $c \in \omega$, $\limsup_{n \rightarrow \infty} \frac{|KR \cap 2^n \setminus SCR_c|}{2^n} > 0$.

Which Π_1^0 sets can be subsets of SCR_c ? Partial answer:

Definition

An infinite set $Q \subseteq 2^{<\omega}$ is **not hyperimmune** if there is a computable function $f: \omega \rightarrow \omega$ such that

$$(\forall n) |Q \cap 2^{\leq f(n)}| \geq n.$$

Theorem

If $Q \subseteq SCR_c$ is an infinite Π_1^0 set, then Q is hyperimmune.

Proposition

For sufficiently large c , there is an infinite Π_1^0 subset of SCR_c .

On the other hand...

Proposition

For sufficiently large c , there is an infinite Π_1^0 subset of SCR_c .

Proposition

For sufficiently large c ,
 $(\exists^\infty n) KR \cap 2^n \subseteq SCR_c$.

On the other hand...

Proposition

For sufficiently large c , there is an infinite Π_1^0 subset of SCR_c .

Proposition

For sufficiently large c ,
 $(\exists^\infty n) KR \cap 2^n \subseteq SCR_c$.

In fact, the set of such n is not even hyperimmune.

Theorem

Let $Q \subseteq 2^{<\omega}$ be a Π_1^0 set such that $(\forall n) Q \cap 2^n \neq \emptyset$. There is a family of strings $\{w_c\}_{c \in \omega} \subseteq Q$ such that:

- 1 $w_c \notin SCR_c$.
- 2 $|w_c| \leq 2^{2^{c+O(\log c)}}$.

Theorem

Let $Q \subseteq 2^{<\omega}$ be a Π_1^0 set such that $(\forall n) Q \cap 2^n \neq \emptyset$. There is a family of strings $\{w_c\}_{c \in \omega} \subseteq Q$ such that:

- 1 $w_c \notin SCR_c$.
- 2 $|w_c| \leq 2^{2^{c+O(\log c)}}$.

This implies Solovay's explicit (and essentially optimal) sequence of counterexamples.

Maximal Complexity—the infinite case

Definition

$A \in 2^\omega$ is **n-random** if it is Martin-Löf random relative to $\emptyset^{(n-1)}$.

Maximal Complexity—the infinite case

Definition

$A \in 2^\omega$ is **n-random** if it is Martin-Löf random relative to $\emptyset^{(n-1)}$.

Definition (Loveland)

$A \in 2^\omega$ is **Kolmogorov random** if
 $(\exists^\infty n) C(A \upharpoonright n) \geq n - O(1)$.

Maximal Complexity—the infinite case

Definition

$A \in 2^\omega$ is **n-random** if it is Martin-Löf random relative to $\emptyset^{(n-1)}$.

Definition (Loveland)

$A \in 2^\omega$ is **Kolmogorov random** if

$$(\exists^\infty n) C(A \upharpoonright n) \geq n - O(1).$$

Studied (in passing) by Martin-Löf, Schnorr and Solovay.

Maximal Complexity—the infinite case

Definition

$A \in 2^\omega$ is **n-random** if it is Martin-Löf random relative to $\emptyset^{(n-1)}$.

Definition (Loveland)

$A \in 2^\omega$ is **Kolmogorov random** if
$$(\exists^\infty n) C(A \upharpoonright n) \geq n - O(1).$$

Studied (in passing) by Martin-Löf, Schnorr and Solovay.

Definition (Solovay)

$A \in 2^\omega$ is **strongly Chaitin random** if
$$(\exists^\infty n) K(A \upharpoonright n) \geq n + K(n) - O(1).$$

Relationships between these classes

Theorem (Solovay)

3-random \implies strongly Chaitin \implies Kolmogorov.

Relationships between these classes

Theorem (Solovay)

3-random \implies strongly Chaitin \implies Kolmogorov.

Theorem (Nies, Stephan, Terwijn)

Kolmogorov random \implies 2-random.

Relationships between these classes

Theorem (Solovay)

3-random \implies strongly Chaitin \implies Kolmogorov.

Theorem (Nies, Stephan, Terwijn)

Kolmogorov random \implies 2-random.

Theorem (Miller; Nies, Stephan, Terwijn)

Kolmogorov random is equivalent to 2-random.

Relationships between these classes

Theorem (Solovay)

3-random \implies strongly Chaitin \implies Kolmogorov.

Theorem (Nies, Stephan, Terwijn)

Kolmogorov random \implies 2-random.

Theorem (Miller; Nies, Stephan, Terwijn)

Kolmogorov random is equivalent to 2-random.

Open Question. Does strongly Chaitin random equal 2-random, 3-random, or neither?

– Thank You –