Higher Randomness and hK-Trivials

Paul-Elliot Anglès d'Auriac
Benoît Monin

March 26, 2019

Randomness in the finite setting

Consider the following game:

Game of Guessing the Random

For every N:

- I choose a sequence in 2^N (deterministically)
- I randomly get another one by throwing N times a coin
- The other player have to bet on which was obtained randomly.

Consider the following game:

Game of Guessing the Random

For every N:

- I choose a sequence in 2^N (deterministically)
- I randomly get another one by throwing N times a coin
- The other player have to bet on which was obtained randomly.

Which sequence would you bet is obtained randomly ?

$$A = 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0$$
$$B = 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0$$

Randomness in the finite setting

Consider the following game:

Game of Guessing the Random

For every N:

- I choose a sequence in 2^N (deterministically)
- I randomly get another one by throwing N times a coin
- The other player have to bet on which was obtained randomly.

Which sequence would you bet is obtained randomly ?

$$A = 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0$$
$$B = 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0$$

However $\mathbf{Pr}(\text{obtaining } A) = \mathbf{Pr}(\text{obtaining } B) = 2^{-11}$...

Randomness in the finite setting

Consider the following game:

Game of Guessing the Random

For every N:

- I choose a sequence in 2^N (deterministically)
- I randomly get another one by throwing N times a coin
- The other player have to bet on which was obtained randomly.

Which sequence would you bet is obtained randomly ?

$$A = 0,0,0,0,0,0,0,0,0,0,0$$
$$B = 0,1,0,0,1,1,1,0,0,1,0$$

However $\mathbf{Pr}(\text{obtaining } A) = \mathbf{Pr}(\text{obtaining } B) = 2^{-11}$...

$$A = 0,1,1,1,0,0,0,1,1,0,0,1,1,1,0,0,1,0,0,0,1...$$
$$B = 0,1,1,0,1,1,0,0,1,0,0,1,0,0,0,0,1,1,0,1,0...$$

A second player strategy

How to compare the randomness of two sequences ? A random sequence is expected to

- Have no structure
- be not predictable,
- be hard to remember
- ...

A second player strategy

How to compare the randomness of two sequences ? A random sequence is expected to

- Have no structure
- be not predictable,
- be hard to remember = being incompressible
- ...

Suppose I moved to 18271852574728528652 8 Logic Street.

Hi Mom!

Please note my new address is 182718525747285286528 Logic Street.

A second player strategy

How to compare the randomness of two sequences ? A random sequence is expected to

- Have no structure
- be not predictable,
- be hard to remember = being incompressible
- ...

Suppose I moved to 100000000000000000000 Logic Street.

Hi Mom!

Please note my new address is "1" and 20 "0" Logic Street.

Formally

Intuition

The more a string is random the bigger is its shortest description (in some coding).

Definition (Kolmogorov Complexity)

$$C(\sigma) = \min\{|\tau| : M(\tau) = \sigma\}$$

where

$$M(0^e 1\sigma) = M_e(\sigma)$$

- 18271852574728528 6528 → $0^{e_{id}}118271852574728528 6528$.
- 10000000000000000000 → $0^e 120$.

Pseudorandomness is not random at all!

Solution

Strategy for the second player

Between A and B, choose the sequence with higher Kolmogorov complexity !

(if you can find it...)

For infinitary sequences

How to measure randomness on infinite sequences ?

$$A = 0101110110100100101101010010101010101010110\ldots$$

When the sequence is infinite, we consider Kolmogorov complexity on prefixes.

[1] Note the switch from C to K a prefix-free version of Kolmogorov complexity, where the size of the program cannot be used as a part of the information...

For infinitary sequences

How to measure randomness on infinite sequences ?

$$A = 0101110110100100101101010010101010101010110\ldots$$

When the sequence is infinite, we consider Kolmogorov complexity on prefixes. Two extremal cases[1] :

Maximal Kolmogorov complexity

$$\forall n, K(A \restriction n) \geq^* n$$

Minimal Kolmogorov complexity

$$\forall n, K(A \restriction n) \leq^* K(n)$$

where $\leq^*$ is inequality up to a constant.

[1] Note the switch from C to K a prefix-free version of Kolmogorov complexity, where the size of the program cannot be used as a part of the information...

ML randomness

Maximal Kolmogorov complexity

A sequence A is called *ML-random* if

$$\forall n, K(A \upharpoonright n) \geq^* n$$

1. We expect such sequences to have no sufficiently simple exceptional property,

Maximal Kolmogorov complexity

A sequence A is called *ML-random* if

$$\forall n, K(A \upharpoonright n) \geq^* n$$

1. We expect such sequences to have no sufficiently simple exceptional property,
2. exceptional properties are $P \subseteq 2^\omega$ with $\lambda(P) = 0$,
3. sufficiently simple properties should include $\{A : \forall n, A(2n) = 0\}$ but not $\{A\}$ for complicated A.

ML randomness

Maximal Kolmogorov complexity

A sequence A is called *ML-random* if

$$\forall n, K(A \upharpoonright n) \geq^* n$$

1. We expect such sequences to have no sufficiently simple exceptional property,
2. exceptional properties are $P \subseteq 2^\omega$ with $\lambda(P) = 0$,
3. sufficiently simple properties should include $\{A : \forall n, A(2n) = 0\}$ but not $\{A\}$ for complicated A.

Characterization (Schnorr)

A is ML-random iff A has no sufficiently simple exceptional property, where:
P is sufficiently simple iff $P = \bigcap \mathcal{U}_n$ where $(\mathcal{U}_n)$ is a family of open, uniformly r.e. sets with $\lambda(\mathcal{U}_n) \leq 2^{-n}$.

K-trivials

Minimal Kolmogorov complexity

A sequence A is called *K-trivial* if

$$\forall n, K(A \upharpoonright n) \leq^* K(n)$$

- Computable sequences are K-trivial,
- but there exist non-computable K-trivials.

K-trivials

Minimal Kolmogorov complexity

A sequence A is called *K-trivial* if

$$\forall n, K(A \upharpoonright n) \leq^* K(n)$$

- Computable sequences are K-trivial,
- but there exist non-computable K-trivials.
- We expect such sequences to have low computational power,

Characterization (Nies, Hirschfeldt)

A sequence A is K-trivial iff ML-randomness=ML^A-randomness.

Higher Randomness

Super-computer Mum

What if we allow more power to decode the description (in K)?

Super-computer Mum

What if we allow more power to decode the description (in K)?

Definition

For a set $A \subseteq \mathbb{N}$, we say that:

1. A is Π^1_1 if there exists a recursive predicate R such that:

$$n \in A \Leftrightarrow \forall X \subseteq \mathbb{N}, \exists m : R(n, m, A),$$

2. A is Σ^1_1 if $\mathbb{N} \setminus A$ is Π^1_1,
3. A is Δ^1_1 if A is both Σ^1_1 and Π^1_1.

Super-computer Mum

What if we allow more power to decode the description (in K)?

Definition

For a set $A \subseteq \mathbb{N}$, we say that:

1. A is Π^1_1 if there exists a recursive predicate R such that:

$$n \in A \Leftrightarrow \forall X \subseteq \mathbb{N}, \exists m : R(n, m, A),$$

2. A is Σ^1_1 if $\mathbb{N} \setminus A$ is Π^1_1,
3. A is Δ^1_1 if A is both Σ^1_1 and Π^1_1.

Definition (higher Kolmogorov Complexity)

$$hK(\sigma) = \min\{|\tau| : M(\tau) = \sigma\}$$

where

Super-computer Mum

What if we allow more power to decode the description (in K)?

Definition

For a set $A \subseteq \mathbb{N}$, we say that:

1. A is Π^1_1 if there exists a recursive predicate R such that:

$$n \in A \Leftrightarrow \forall X \subseteq \mathbb{N}, \exists m : R(n, m, A),$$

2. A is Σ^1_1 if $\mathbb{N} \setminus A$ is Π^1_1,
3. A is Δ^1_1 if A is both Σ^1_1 and Π^1_1.

Definition (higher Kolmogorov Complexity)

$$hK(\sigma) = \min\{|\tau| : M(\tau) = \sigma\}$$

where

M is a universal prefix-free Π^1_1 machine

Why Π^1_1?

Recall that

Fact

A is r.e. iff $(n \in A \Leftrightarrow \exists t : \phi_e(n)[t])$.

It's a Σ^0_1 statement. Shouldn't we choose Σ^1_1 in our higher K?

Why Π^1_1?

Recall that

Fact

A is r.e. iff $(n \in A \Leftrightarrow \exists t : \phi_e(n)[t])$.

It's a Σ^0_1 statement. Shouldn't we choose Σ^1_1 in our higher K?

Theorem

$\mathcal{O} = \{e : \phi_e$ *codes a well order*$\}$ *is* Π^1_1*-complete, i.e if* A *is* Π^1_1*, then for some recursive* f*:*

$$n \in A \Leftrightarrow f(n) \in \mathcal{O}.$$

Why Π^1_1?

Recall that

Fact

A is r.e. iff $(n \in A \Leftrightarrow \exists t : \phi_e(n)[t])$.

It's a Σ^0_1 statement. Shouldn't we choose Σ^1_1 in our higher K?

Theorem

$\mathcal{O} = \{e : \phi_e$ *codes a well order*$\}$ *is* Π^1_1*-complete, i.e if* A *is* Π^1_1*, then for some recursive* f*:*

$$n \in A \Leftrightarrow f(n) \in \mathcal{O}.$$

1. We can slice $\mathcal{O} = \bigcup_{\alpha < \omega_1^{CK}} \mathcal{O}_\alpha$,
2. Then $A = \bigcup_{\alpha < \omega_1^{CK}} A_\alpha$ where $n \in A_\alpha \Leftrightarrow f(n) \in \mathcal{O}_\alpha$
3. $(A_\alpha)_{\alpha < \omega_1^{CK}}$ is an increasing union of uniformly Δ^1_1 sets, along computable ordinals.

I don't like technical talks

1. We have a new notion of computation, with time going along computable ordinals,
2. we plugged this in our definition of K, giving us hK

Now, routine:

I don't like technical talks

1. We have a new notion of computation, with time going along computable ordinals,
2. we plugged this in our definition of K, giving us hK

Now, routine:

Minimal higher Kolmogorov complexity

A sequence A is called *hK-trivial* if

$$\forall n, hK(A \upharpoonright n) \leq^* hK(n)$$

Maximal Kolmogorov complexity

A sequence A is called Π^1_1*-ML-random* if

$$\forall n, hK(A \upharpoonright n) \geq^* n$$

Question

Do Π^1_1-ML-randoms have the same kind of properties as ML-randoms?

Question

Do hK-trivials have the same kind of properties as K-trivials?

Question

What about the other notions from algorithmic randomness?

Some answers are already known:

Characterization (Bienvenu, Greenberg, Monin)

A is Π^1_1-ML-random iff A has no sufficiently simple exceptional property, where:
P is sufficiently simple iff $P = \bigcap \mathcal{U}_n$ where $(\mathcal{U}_n)$ is a family of open, uniformly Π^1_1. sets with $\lambda(\mathcal{U}_n) \leq 2^{-n}$.

Characterization (Bienvenu, Greenberg, Monin)

A sequence A is hK-trivial iff
Π^1_1-ML-randomness=Π^1_1-ML^A-randomness.

Some results

Some answers are already known:

Characterization (Bienvenu, Greenberg, Monin)

A is Π^1_1-ML-random iff A has no sufficiently simple exceptional property, where:
P is sufficiently simple iff $P = \bigcap \mathcal{U}_n$ where $(\mathcal{U}_n)$ is a family of open, uniformly Π^1_1. sets with $\lambda(\mathcal{U}_n) \leq 2^{-n}$.

Characterization (Bienvenu, Greenberg, Monin)

A sequence A is hK-trivial iff
Π^1_1-ML-randomness=Π^1_1-ML^A-randomness.

Now let's get straight to our result!

Definition (Weak-2-Randomness, Weak-Π^1_1-Randomness)

A is W2R if A has no Π^0_2 exceptional property, and WΠ^1_1R for the higher counterpart.

Definition (Martin-Löf$\langle 0' \rangle$, Π^1_1-Martin-Löf$\langle \mathcal{O} \rangle$)

A property $P = \bigcap_n \mathcal{U}_{f(n)}$ is a ML$\langle 0' \rangle$ test if $f \leq 0'$ and $\lambda(\mathcal{U}_{f(n)}) \leq 2^{-n}$. A set A is ML$\langle 0' \rangle$-random if it is in no ML$\langle 0' \rangle$ test. Π^1_1-ML$\langle \mathcal{O} \rangle$-randomness is the higher conterpart.

Definition (Weak-2-Randomness, Weak-Π^1_1-Randomness)

A is W2R if A has no Π^0_2 exceptional property, and $W\Pi^1_1R$ for the higher counterpart.

Definition (Martin-Löf$\langle 0' \rangle$, Π^1_1-Martin-Löf$\langle \mathcal{O} \rangle$)

A property $P = \bigcap_n \mathcal{U}_{f(n)}$ is a ML$\langle 0' \rangle$ test if $f \leq 0'$ and $\lambda(\mathcal{U}_{f(n)}) \leq 2^{-n}$. A set A is ML$\langle 0' \rangle$-random if it is in no ML$\langle 0' \rangle$ test. Π^1_1-ML$\langle \mathcal{O} \rangle$-randomness is the higher conterpart.

Theorem (Nies ; Kjos-Hanssen, Miller, and Solomon)

A is K-trivial if and only if

$$\mathrm{W2R}^A = \mathrm{W2R} = \mathrm{ML}\langle 0' \rangle$$

Theorem (Monin)

$$\mathrm{W}\Pi^1_1\mathrm{R} \neq \mathrm{ML}\langle \mathcal{O} \rangle$$

Our result

Theorem (Nies ; Kjos-Hanssen, Miller, and Solomon)

A is K-trivial if and only if

$$\mathrm{W2R} = \mathrm{W2R}^{A} = \mathrm{ML}\langle 0' \rangle$$

Theorem (Monin)

$$\mathrm{W}\Pi^1_1\mathrm{R} \supsetneq \Pi^1_1\text{-}\mathrm{ML}\langle \mathcal{O} \rangle$$

Our result

Theorem (Nies ; Kjos-Hanssen, Miller, and Solomon)

A is K-trivial if and only if

$$\mathrm{W2R} = \mathrm{W2R}^A = \mathrm{ML}\langle 0' \rangle$$

Theorem (Monin)

$$\mathrm{W}\Pi^1_1\mathrm{R} \supsetneq \Pi^1_1\text{-}\mathrm{ML}\langle \mathcal{O} \rangle$$

- If A is hK-trivial, then where is $\mathrm{W}\Pi^1_1\mathrm{R}^A$?
- When A is Δ^1_1, we have $\mathrm{W}\Pi^1_1\mathrm{R} = \mathrm{W}\Pi^1_1\mathrm{R}^A$. Otherwise...

Our result

Theorem (Nies ; Kjos-Hanssen, Miller, and Solomon)

A is K-trivial if and only if

$$\mathrm{W2R} = \mathrm{W2R}^A = \mathrm{ML}\langle 0' \rangle$$

Theorem (Monin)

$$\mathrm{W}\Pi^1_1\mathrm{R} \supsetneq \Pi^1_1\text{-}\mathrm{ML}\langle \mathcal{O} \rangle$$

- If A is hK-trivial, then where is $\mathrm{W}\Pi^1_1\mathrm{R}^A$?
- When A is Δ^1_1, we have $\mathrm{W}\Pi^1_1\mathrm{R} = \mathrm{W}\Pi^1_1\mathrm{R}^A$. Otherwise...

Theorem (A., Monin)

A is hK-trivial not Δ^1_1 if and only if

$$\mathrm{W}\Pi^1_1\mathrm{R}^A = \Pi^1_1\text{-}\mathrm{ML}\langle \mathcal{O} \rangle$$

Conclusion

Theorem

$$\mathrm{W}\Pi^1_1\mathrm{R} \supsetneq \mathrm{ML}\langle\mathcal{O}\rangle$$

Theorem

A is hK-trivial not Δ^1_1 if and only if

$$\mathrm{W}\Pi^1_1\mathrm{R}^A = \Pi^1_1\text{-}\mathrm{ML}\langle\mathcal{O}\rangle$$

A characterization of non (higher-)computable hK-Trivial that has no equivalent on the lower setting.

Conclusion

Theorem

$$\mathrm{W}\Pi^1_1\mathrm{R} \supsetneq \mathrm{ML}\langle\mathcal{O}\rangle$$

Theorem

A is hK-trivial not Δ^1_1 if and only if

$$\mathrm{W}\Pi^1_1\mathrm{R}^A = \Pi^1_1\text{-}\mathrm{ML}\langle\mathcal{O}\rangle$$

A characterization of non (higher-)computable hK-Trivial that has no equivalent on the lower setting.

Thank you for your attention!