The axiomatic power of Kolmogorov complexity

Antoine Taveneaux
[with L. Bienvenu, A. Romashchenko, A. Shen and S. Vermeeren]

LIAFA

Journées Calculabilités
March 6, 2012

Plan

Plan

Kolmogorov complexity

- The Kolmogorov complexity of x is the length of the shortest program with output x :

$$\mathrm{C}_T(x) = \{n \mid \exists p \ |p| = n \text{ and } T(p) = x\}$$

Kolmogorov complexity

- The Kolmogorov complexity of x is the length of the shortest program with output x :

$$\mathrm{C}_T(x) = \{n \mid \exists p \ |p| = n \text{ and } T(p) = x\}$$

- There is an optimal machine U such that for any other machine T there is a constant d_T such that for all x :

$$\mathrm{C}_U(x) \leq \mathrm{C}_T(c) + d_T$$

Kolmogorov complexity

- The Kolmogorov complexity of x is the length of the shortest program with output x :

$$\mathrm{C}_T(x) = \{n \mid \exists p \ |p| = n \text{ and } T(p) = x\}$$

- There is an optimal machine U such that for any other machine T there is a constant d_T such that for all x :

$$\mathrm{C}_U(x) \leq \mathrm{C}_T(c) + d_T$$

- Then we define complexity C by $\mathrm{C} = \mathrm{C}_U$

Kolmogorov complexity

- The Kolmogorov complexity of x is the length of the shortest program with output x :

$$\mathrm{C}_T(x) = \{n \mid \exists p \ |p| = n \text{ and } T(p) = x\}$$

- There is an optimal machine U such that for any other machine T there is a constant d_T such that for all x :

$$\mathrm{C}_U(x) \leq \mathrm{C}_T(c) + d_T$$

- Then we define complexity C by $\mathrm{C} = \mathrm{C}_U$
- For prefix free machine the situation is the same. Then we can define prefix free complexity K with an optimal prefix free machines.

Gödel theorem with Kolmogorov complexity

Theorem (Chaitin)

Peano arithmetic is consistent can prove sentences of the form

$$\mathrm{C}(x) \geq n$$

only for a finite number of n.

Gödel theorem with Kolmogorov complexity

Theorem (Chaitin)

Peano arithmetic is consistent can prove sentences of the form

$$\mathrm{C}(x) \geq n$$

only for a finite number of n.

Proof

- *It is an adaptation of Berry's paradox.*

Gödel theorem with Kolmogorov complexity

Theorem (Chaitin)

Peano arithmetic is consistent can prove sentences of the form

$$\mathrm{C}(x) \geq n$$

only for a finite number of n.

Proof

- *It is an adaptation of Berry's paradox.*
- *Suppose that for any n we can find x such that Peano arithmetic proves* $\mathrm{C}(x) \geq n$

Gödel theorem with Kolmogorov complexity

Theorem (Chaitin)

Peano arithmetic is consistent can prove sentences of the form

$$\mathrm{C}(x) \geq n$$

only for a finite number of n.

Proof

- *It is an adaptation of Berry's paradox.*
- *Suppose that for any n we can find x such that Peano arithmetic proves $\mathrm{C}(x) \geq n$*
- *Then with a program of length $d + \log(n)$ we can find the first string y such that Peano arithmetic proves $\mathrm{C}(y) \geq n$ ...*

Gödel theorem with Kolmogorov complexity

Theorem (Chaitin)

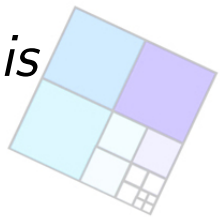
Peano arithmetic is consistent can prove sentences of the form

$$\mathrm{C}(x) \geq n$$

only for a finite number of n.

Proof

- *It is an adaptation of Berry's paradox.*
- *Suppose that for any n we can find x such that Peano arithmetic proves* $\mathrm{C}(x) \geq n$
- *Then with a program of length* $d + \log(n)$ *we can find the first string y such that Peano arithmetic proves* $\mathrm{C}(y) \geq n$ *. . .But this short program outputs a string with complexity larger than n*



Plan

Random axioms

- For N large enough $\mathrm{C}(x) \geq N$ is not provable

Random axioms

- For N large enough $\mathrm{C}(x) \geq N$ is not provable
- If we chose at random string x of length n then $\mathrm{C}(x) \geq n - k$ is true with probability bigger than $1 - 2^{-k}$

Random axioms

- For N large enough $\mathrm{C}(x) \geq N$ is not provable
- If we chose at random string x of length n then $\mathrm{C}(x) \geq n - k$ is true with probability bigger than $1 - 2^{-k}$
- Then we can toss a coin $N + 100$ times to get $x \in 2^{<\omega}$ and add the axiom $\mathrm{C}(x) \geq N$ to Peano arithmetic

Random axioms

- For N large enough $\mathrm{C}(x) \geq N$ is not provable
- If we chose at random string x of length n then $\mathrm{C}(x) \geq n - k$ is true with probability bigger than $1 - 2^{-k}$
- Then we can toss a coin $N + 100$ times to get $x \in 2^{<\omega}$ and add the axiom $\mathrm{C}(x) \geq N$ to Peano arithmetic
- Then we get a stronger theory

Random axioms

- For N large enough $\mathrm{C}(x) \geq N$ is not provable
- If we chose at random string x of length n then $\mathrm{C}(x) \geq n - k$ is true with probability bigger than $1 - 2^{-k}$
- Then we can toss a coin $N + 100$ times to get $x \in 2^{<\omega}$ and add the axiom $\mathrm{C}(x) \geq N$ to Peano arithmetic
- Then we get a stronger theory. . .can we prove the consistency of Peano arithmetic with this new theory ?

A more abstract vision

- More generally we can add more than one axiom :

  $\mathrm{C}(x_1) \geq |x_1| - 100$ and $\mathrm{C}(x_2) \geq |x_2| - 100$ and $\ldots \mathrm{C}(x_k) \geq |x_k| - 100$

A more abstract vision

- More generally we can add more than one axiom :

  $\mathrm{C}(x_1) \geq |x_1| - 100$ and $\mathrm{C}(x_2) \geq |x_2| - 100$ and $\ldots \mathrm{C}(x_k) \geq |x_k| - 100$

- For some rational $\delta > 0$ and property $R(x)$ with one free variable such that the number of strings x of length N such that $\neg R(x)$ does not exceed $\delta 2^N$

A more abstract vision

- More generally we can add more than one axiom :

  $\mathrm{C}(x_1) \geq |x_1| - 100$ and $\mathrm{C}(x_2) \geq |x_2| - 100$ and $\ldots \mathrm{C}(x_k) \geq |x_k| - 100$

- For some rational $\delta > 0$ and property $R(x)$ with one free variable such that the number of strings x of length N such that $\neg R(x)$ does not exceed $\delta 2^N$
  - Then we can toss a fair coin N times to get x of length N and add the formula $R(x)$ as a new axiom

A more abstract vision

- More generally we can add more than one axiom :

  $\mathrm{C}(x_1) \geq |x_1| - 100$ and $\mathrm{C}(x_2) \geq |x_2| - 100$ and $\ldots \mathrm{C}(x_k) \geq |x_k| - 100$

- For some rational $\delta > 0$ and property $R(x)$ with one free variable such that the number of strings x of length N such that $\neg R(x)$ does not exceed $\delta 2^N$
  - Then we can toss a fair coin N times to get x of length N and add the formula $R(x)$ as a new axiom, and we say that we have to pay a capital δ (because the probability to say something wrong is at most δ)

A more abstract vision

- More generally we can add more than one axiom :

  $\mathrm{C}(x_1) \geq |x_1| - 100$ and $\mathrm{C}(x_2) \geq |x_2| - 100$ and $\ldots \mathrm{C}(x_k) \geq |x_k| - 100$

- For some rational $\delta > 0$ and property $R(x)$ with one free variable such that the number of strings x of length N such that $\neg R(x)$ does not exceed $\delta 2^N$
  - Then we can toss a fair coin N times to get x of length N and add the formula $R(x)$ as a new axiom, and we say that we have to pay a capital δ (because the probability to say something wrong is at most δ)
  - We can repeat this several times

A more abstract vision

- More generally we can add more than one axiom :

  $\mathrm{C}(x_1) \geq |x_1| - 100$ and $\mathrm{C}(x_2) \geq |x_2| - 100$ and $\ldots \mathrm{C}(x_k) \geq |x_k| - 100$

- For some rational $\delta > 0$ and property $R(x)$ with one free variable such that the number of strings x of length N such that $\neg R(x)$ does not exceed $\delta 2^N$
  - Then we can toss a fair coin N times to get x of length N and add the formula $R(x)$ as a new axiom, and we say that we have to pay a capital δ (because the probability to say something wrong is at most δ)
  - We can repeat this several times, for each operation we pay δ until the initial capital ε is exhausted

Soundness

Theorem

Let ψ be some arithmetical statement. If the probability to prove ψ for a proof strategy π with initial capital ε is greater than ε, then ψ is true.

Soundness

Theorem

Let ψ be some arithmetical statement. If the probability to prove ψ for a proof strategy π with initial capital ε is greater than ε, then ψ is true.

- Then no contradiction can appear with probability bigger than ε

Soundness

Theorem

Let ψ be some arithmetical statement. If the probability to prove ψ for a proof strategy π with initial capital ε is greater than ε, then ψ is true.

- Then no contradiction can appear with probability bigger than ε
- This game is not too dangerous . . .

Conservation

Theorem

Let ψ be some arithmetical statement. If the probability to prove ψ for a proof strategy π with initial capital ε is greater than ε, then ψ is provable (in PA *without any additional axioms).*

Conservation

Theorem

Let ψ be some arithmetical statement. If the probability to prove ψ for a proof strategy π with initial capital ε is greater than ε, then ψ is provable (in PA *without any additional axioms).*

- In other words, if you try to prove something true but non-provable then it is useless to use this kind of proof strategy

Conservation

Theorem

Let ψ be some arithmetical statement. If the probability to prove ψ for a proof strategy π with initial capital ε is greater than ε, then ψ is provable (in PA *without any additional axioms).*

- In other words, if you try to prove something true but non-provable then it is useless to use this kind of proof strategy
- And if we add false but non provable axioms ?

Plan

Axioms about Kolmogorov complexity

- What happens if we add a large part of true formulas of the form

$$\mathrm{C}(x) \geq n\,?$$

Axioms about Kolmogorov complexity

- What happens if we add a large part of true formulas of the form

$$\mathrm{C}(x) \geq n\,?$$

- What happens if we add all true formulas of the form

$$\mathrm{C}(x) \geq n\,?$$

All information about Kolmogorov complexity

Theorem

If, in PA, *we add as axioms all true statement of the form*

$$\mathrm{C}(x) \geq |x|$$

The resulting theory is PA *plus all true* Π_1*-statements*

All information about Kolmogorov complexity

Theorem

If, in PA, *we add as axioms all true statement of the form*

$$\mathrm{C}(x) \geq |x|$$

The resulting theory is PA *plus all true* Π_1*-statements*

- For example we can show the consistency of PA in this system.

All information about Kolmogorov complexity

Theorem

If, in PA, *we add as axioms all true statement of the form*

$$\mathrm{C}(x) \geq |x|$$

The resulting theory is PA *plus all true* Π_1*-statements*

- For example we can show the consistency of PA in this system.

Proof

This is mainly an effective version of the reduction of the halting problem to the function C*.*

Most information about Kolmogorov complexity

Most information about Kolmogorov complexity

Theorem

Let ψ be an Π_1-unprovable statement.
There is a set A with 99% (for each length) of strings x such that $\mathrm{C}(x) \geq |x|$ and such that theory PA *plus all axiom $\mathrm{C}(x) \geq |x|$ for x in* PA *does not prove ψ*

Most information about Kolmogorov complexity

Theorem

Let ψ be an Π_1-unprovable statement.
There is a set A with 99% (for each length) of strings x such that $\mathrm{C}(x) \geq |x|$ and such that theory PA *plus all axiom $\mathrm{C}(x) \geq |x|$ for x in* PA *does not prove ψ*

Proof

By induction (on the length of strings x) we show that if the previous theorem does not hold then ψ is provable from too many random axioms.

Less is more ?

Theorem

There is a sequence of string (x_n) *such that for all* n *we have* $|x_n| = n$ *and* $\mathrm{C}(x_n) \geq n$ *is true and if we add all axioms* $\mathrm{C}(x_n) \geq n$ *to* PA *then we get* PA *plus all true* Π_1*-statements*

Less is more ?

Theorem

There is a sequence of string (x_n) *such that for all* n *we have* $|x_n| = n$ *and* $\mathrm{C}(x_n) \geq n$ *is true and if we add all axioms* $\mathrm{C}(x_n) \geq n$ *to* PA *then we get* PA *plus all true* Π_1*-statements*

Proof

If x_n *is the left most string of length* n *such that* $\mathrm{C}(x_n) \geq n$ *then with this axiom we can find (and prove that this number has this property) a waiting time* t *such that all program of length less than* n *halt in time less than* t*.*

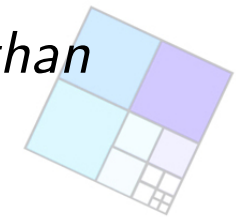
Less is more ?

Theorem

There is a sequence of string (x_n) *such that for all* n *we have* $|x_n| = n$ *and* $\mathrm{C}(x_n) \geq n$ *is true and if we add all axioms* $\mathrm{C}(x_n) \geq n$ *to* PA *then we get* PA *plus all true* Π_1*-statements*

Proof

If x_n *is the left most string of length* n *such that* $\mathrm{C}(x_n) \geq n$ *then with this axiom we can find (and prove that this number has this property) a waiting time* t *such that all program of length less than* n *halt in time less than* t*.*
Then with this t *we can decide any* Π_1*-statement of length less than* $n - O(1)$*.*



Just one constant

Theorem

There exists some constant c such that PA *together with all true statements of the type $\mathrm{C}(x|y) \geq c$ proves all true Π_1-statements.*

What are these useful axioms ?

- As seen before some axioms $\mathrm{C}(x) \geq |x|$ allow us to decide all Π_1-statement of length less than $|x| - O(1)$

What are these useful axioms ?

- As seen before some axioms $\mathrm{C}(x) \geq |x|$ allow us to decide all Π_1-statement of length less than $|x| - O(1)$
- In some sense this phenomenon is accidental because most strings do not have this property

What are these useful axioms ?

- As seen before some axioms $\mathrm{C}(x) \geq |x|$ allow us to decide all Π_1-statement of length less than $|x| - O(1)$
- In some sense this phenomenon is accidental because most strings do not have this property
- How can we characterise these strings ?

What are these useful axioms ?

- As seen before some axioms $\mathrm{C}(x) \geq |x|$ allow us to decide all Π_1-statement of length less than $|x| - O(1)$
- In some sense this phenomenon is accidental because most strings do not have this property
- How can we characterise these strings ? The utility of a string x could be related to $\mathrm{C}^{\emptyset'}(x) - \mathrm{C}(x)$

The same axiom with a partial information

- Take a string x such that $\mathrm{C}(x) \geq |x|$ is true and allow us to decide all Π_1-statement of length less than $|x| - O(1)$

The same axiom with a partial information

- Take a string x such that $\mathrm{C}(x) \geq |x|$ is true and allow us to decide all Π_1-statement of length less than $|x| - O(1)$

- What can we prove with the weaker axiom $\mathrm{C}(x) \geq |x|/2$?

The same axiom with a partial information

- Take a string x such that $\mathrm{C}(x) \geq |x|$ is true and allow us to decide all Π_1-statement of length less than $|x| - O(1)$

- What can we prove with the weaker axiom $\mathrm{C}(x) \geq |x|/2$? We can show that this axiom does not allow us to decide all Π_1-statement of length less than $|x|/2 - O(1)$

The same axiom with a partial information

- Take a string x such that $\mathrm{C}(x) \geq |x|$ is true and allow us to decide all Π_1-statement of length less than $|x| - O(1)$
- What can we prove with the weaker axiom $\mathrm{C}(x) \geq |x|/2$? We can show that this axiom does not allow us to decide all Π_1-statement of length less than $|x|/2 - O(1)$
- Towards a semantic reduction ?

Plan

PA plus a random sequence

- A sequence $X \in 2^\omega$ is Martin-Löf random if there is c such that

$$\mathrm{K}(X \upharpoonright n) \geq n - c$$

PA plus a random sequence

- A sequence $X \in 2^\omega$ is Martin-Löf random if there is c such that

$$\mathrm{K}(X \upharpoonright n) \geq n - c$$

- If we add all axioms $\mathrm{K}(X \upharpoonright n) \geq n - c$ to PA what theory do we get ?

PA plus a random sequence

- A sequence $X \in 2^\omega$ is Martin-Löf random if there is c such that

$$\mathrm{K}(X \upharpoonright n) \geq n - c$$

- If we add all axioms $\mathrm{K}(X \upharpoonright n) \geq n - c$ to PA what theory do we get ?

- In the sequels $\mathrm{MLR}_c(X)$ denotes PA plus all axioms $\mathrm{K}(X \upharpoonright n) \geq n - c$

Is c important ?

- If $\mathrm{MLR}_c(X)$ is consistent and proves ψ is it true that $\mathrm{MLR}_{c+1}(X)$ must proves ψ ?

Is c important ?

- If $\mathrm{MLR}_c(X)$ is consistent and proves ψ is it true that $\mathrm{MLR}_{c+1}(X)$ must proves ψ ?

Theorem

Let X be a Martin-Löf random sequence. If ψ is provable in all theories $\mathrm{MLR}_c(X)$, then ψ is provable in PA.

Is c important ?

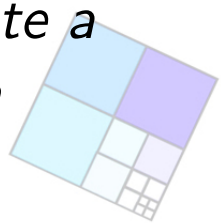
- If $\mathrm{MLR}_c(X)$ is consistent and proves ψ is it true that $\mathrm{MLR}_{c+1}(X)$ must proves ψ ?

Theorem

Let X be a Martin-Löf random sequence. If ψ is provable in all theories $\mathrm{MLR}_c(X)$, then ψ is provable in PA.

Proof

The proof uses the fact the set of axioms proving ψ (if ψ is not provable in PA*) has small measure and from this fact we can create a Martin-Löf test (with parameter c) showing that X is not random*



Is there powerful Martin-Löf random sequence ?

Theorem

If the theory $\mathrm{MLR}_c(X)$ *is consistent, it does not prove all true universal statements.*

Is there powerful Martin-Löf random sequence ?

Theorem

If the theory $\mathrm{MLR}_c(X)$ *is consistent, it does not prove all true universal statements.*

Proof

- *The proof use advanced technical tools from recursion theory*

Is there powerful Martin-Löf random sequence ?

Theorem

If the theory $\mathrm{MLR}_c(X)$ *is consistent, it does not prove all true universal statements.*

Proof

- *The proof use advanced technical tools from recursion theory*
- *We create a incomplete (in the Turing sense) set of strings A such that for all n we have* $X \upharpoonright n \in A$ *ans for all* $x \in A$ *we have* $\mathrm{K}(x) \geq |x| - c$

More than a random sequence

Theorem

For some sequence $X \in 2^\omega$, if we add axioms "$\mathrm{K}(X \upharpoonright n) \geq n - c$ and $X \upharpoonright n$ can be continued in a random string with a deficiency c"
This theory can decide all Π_1-statements

More than a random sequence

Theorem

For some sequence $X \in 2^\omega$, if we add axioms "$\mathbb{K}(X \upharpoonright n) \geq n - c$ and $X \upharpoonright n$ can be continued in a random string with a deficiency c"
This theory can decide all Π_1-statements

Proof

If X is a left most path in sequences with deficiency c then if we know that $X \upharpoonright n$ can be continued in a random string with a deficiency c we can prove that X is a left most path in sequences with deficiency c. And this implies that X is a Chaitin's Ω number and from that we can provably decide which programs halt.

K-triviality

- a sequence $X \in 2^\omega$ is K-trivial if there is c such that for all n we have

$$\mathrm{K}(X \upharpoonright n) \leq \mathrm{K}(n) + c$$

K-triviality

- a sequence $X \in 2^\omega$ is K-trivial if there is c such that for all n we have
$$\mathrm{K}(X \upharpoonright n) \leq \mathrm{K}(n) + c$$

- Some K-trivial sequences are not computable (Solovay)

K-triviality

- a sequence $X \in 2^\omega$ is K-trivial if there is c such that for all n we have
$$\mathrm{K}(X \upharpoonright n) \leq \mathrm{K}(n) + c$$

- Some K-trivial sequences are not computable (Solovay)

- But the set
$$\{X \in 2^\omega | \exists c \forall n \ \mathrm{PA} \vdash \mathrm{K}(X \upharpoonright n) \leq \mathrm{K}(n) + c\}$$

K-triviality

- a sequence $X \in 2^\omega$ is K-trivial if there is c such that for all n we have
$$\mathrm{K}(X \upharpoonright n) \leq \mathrm{K}(n) + c$$

- Some K-trivial sequences are not computable (Solovay)

- But the set
$$\{X \in 2^\omega | \exists c \forall n \ \mathrm{PA} \vdash \mathrm{K}(X \upharpoonright n) \leq \mathrm{K}(n) + c\}$$
is exactly the set of computable sequences

Another vision of K-triviality

- It is not the only way to define what is a K-trivial sequence

Another vision of K-triviality

- It is not the only way to define what is a K-trivial sequence

- Bienvenu, Downey, Merkle and Nies have showen that there is a computable function $f : 2^{<\omega} \to \mathbb{N}$ such that $X \in 2^{\omega}$ is K-trivial if and only if there is c such that for all n we have

$$\mathrm{K}(X \upharpoonright n) \leq f(n) + c$$

Another vision of K-triviality

- It is not the only way to define what is a K-trivial sequence
- Bienvenu, Downey, Merkle and Nies have showen that there is a computable function $f : 2^{<\omega} \to \mathbb{N}$ such that $X \in 2^{\omega}$ is K-trivial if and only if there is c such that for all n we have

$$\mathrm{K}(X \upharpoonright n) \leq f(n) + c$$

- The last statement is Σ_1 and thus provable.

Another vision of K-triviality

- It is not the only way to define what is a K-trivial sequence
- Bienvenu, Downey, Merkle and Nies have showen that there is a computable function $f : 2^{<\omega} \to \mathbb{N}$ such that $X \in 2^{\omega}$ is K-trivial if and only if there is c such that for all n we have

$$\mathrm{K}(X \upharpoonright n) \leq f(n) + c$$

- The last statement is Σ_1 and thus provable.
- The way to express a property can be very important in the provability world

Program generating an Ω

- In the c.e. case, other way to think about infinite sequences : Calude proved that if X is left-c.e. random, then there exists e such that X is left-c.e. random of index e and PA proves "the left-c.e. real of index e is random"

Program generating an Ω

- In the c.e. case, other way to think about infinite sequences : Calude proved that if X is left-c.e. random, then there exists e such that X is left-c.e. random of index e and PA proves "the left-c.e. real of index e is random"

- Can we do the same for c.e. K-trivial ?

¿ Questions ?