The truth-table completeness of Kolmogorov complexity

Nils Lauermann

Advisor: Fabian Kunze

Programming Systems Lab
Saarland University

May 20, 2021

History: Kolmogorov complexity

1960

A PRELIMINARY REPORT ON
A GENERAL THEORY
OF INDUCTIVE INFERENCE

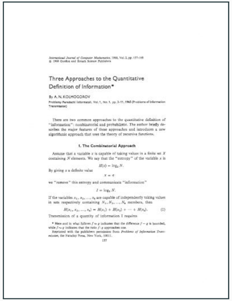
R. J. Solomonoff

Abstract

"A preliminary report on a general theory of inductive inference."

Ray J. Solomonoff

1965



Three Approaches to the Quantitative
Definition of Information*

By A. N. KOLMOGOROV

1. The Combinatorial Approach

"Three approaches to the quantitative definition of information."

Andrey N. Kolmogorov

1996

On the Complexity of Random Strings
(Extended Abstract)

Martin Kummer

1 Introduction

"On the complexity of random strings."

Martin Kummer

Definitions

What is a truth-table reduction?

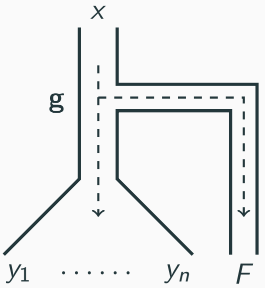
Many-one reduction

f: $X \to Y$

$$A \leqslant_m B \Leftrightarrow (x \in A \Leftrightarrow f(x) \in B)$$

Truth-table reduction

g: $X \to \mathbb{L}Y \times (\mathbb{LB} \to \mathbb{B})$



$$A \leqslant_{tt} B \Leftrightarrow (x \in A \Leftrightarrow F\ [\ulcorner y_1 \in B \urcorner, \dots, \ulcorner y_n \in B \urcorner])$$

Basic definitions I

Definition: numbering ψ

$$\psi : \underbrace{\mathbb{N}}_{\text{program}} \times \underbrace{\mathbb{N}}_{\text{input}} \rightarrow \underbrace{\mathbb{N}}_{\text{output}}$$

Definition: Kolmogorov complexity $C_\psi : \mathbb{N} \rightarrow \mathbb{N} \cup \{\infty\}$

$$C_\psi(x) = \min\{\text{length}(p) \mid \psi(p, 0) = x\}$$

Basic definitions II

Definition: The set of non-random numbers $\overline{R_\psi}$

$$\overline{R_\psi} = \{x \mid C_\psi(x) < \text{length}(x)\}$$

Definition: $M_{n,s}$ - The set of step-limited non-random numbers of length n

$$M_{n,s} = \{\sigma \in \{0,1\}^n \mid \sigma \in \overline{R_\psi} \wedge \psi \text{ terminated in } s \text{ steps}\}$$

$\overline{R_\psi}$ is truth-table complete

Fact: $\overline{R_\psi} \in RE$

For input x try all programs p with $\text{length}(p) < \text{length}(x)$ for increasingly more steps.

Theorem[1]**:** $\forall E \in RE.\ E \leqslant_{tt} \overline{R_\psi}$

ψ must be an optimal numbering i.e. can efficiently simulate any other numbering.

[1] [Kummer, 1996]

Kummer’s proof

Preliminaries

Theorem[1]: $\forall E \in RE.\ E \leqslant_{tt} \overline{R_\psi}$

Definition: E_s

The set of elements enumerated into E before step s

Now, the algorithm to construct the reduction function

[1] [Kummer, 1996]

Step 0

S_0

$\vdots$

$\vdots$

$\vdots$

$S_{i_{max}}$

Step 1

S_0

$\vdots$

S_i | $\{\cdots\} \subseteq \mathbb{N}$

$\vdots$

$S_{i_{max}}$

Step s

S_0	$\{\cdots\}\ \{\cdots\}\ \{\cdots\}$
$\vdots$	
S_i	$\{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}$
$\vdots$	
$S_{i_{max}}$	$\{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}$

Step s

S_0	$\{\cdots\}\ \{\cdots\}\ \{\cdots\}$
$\vdots$	
S_i	$\{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}$
$\vdots$	
$S_{i_{max}}$	$\{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}$

Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$$i * c(n) \leqslant |M_{n,s}|$$

Step s

$$
\begin{array}{r|l}
S_0 & \{\cdots\}\ \{\cdots\}\ \{\cdots\} \\
\vdots & \\
\to S_i & \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\} \\
\vdots & \\
S_{i_{max}} & \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}
\end{array}
$$

Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$$i * c(n) \leqslant |M_{n,s}|$$

Step s

S_0 | $\{\cdots\}\ \{\cdots\}\ \{\cdots\}$

$\vdots$

$\rightarrow S_i$ | $\{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}$

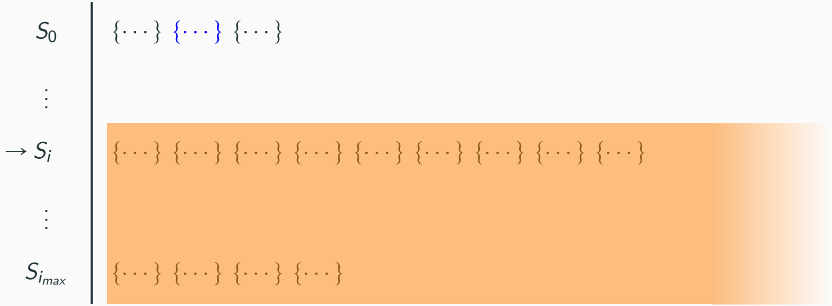
$\vdots$

$S_{i_{max}}$ | $\{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}$

Choose greatest i $(\leqslant i_{max})$ and then smallest n $(\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in •

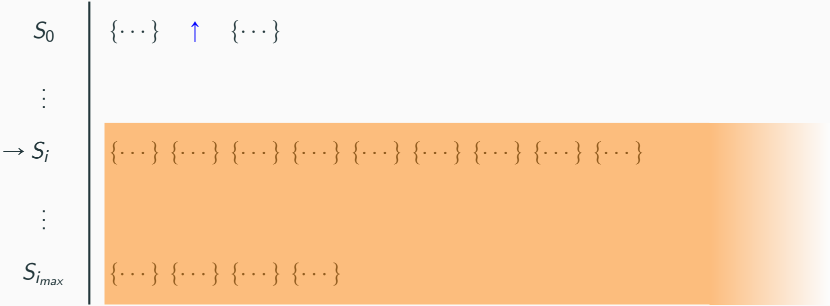
Step s



Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in •

Step s



Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in •

Step s

S_0	$\{\cdots\}$ $\uparrow$ $\{\cdots\}$
$\vdots$	
$\rightarrow S_i$	$\{\cdots\}$ $\{\cdots\}$ $\{\cdots\}$ $\{\cdots\}$ $\{\cdots\}$ $\{\cdots\}$ $\{\cdots\}$ $\{\cdots\}$ $\{\cdots\}$ $S_{i,k}$
$\vdots$	
$S_{i_{max}}$	$\{\cdots\}$ $\{\cdots\}$ $\{\cdots\}$ $\{\cdots\}$

Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in •

Step s

$$
\begin{array}{r|l}
S_0 & \{\cdots\} \quad \uparrow \quad \{\cdots\} \\
\vdots & \\
\rightarrow S_i & \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\} \quad S_{i,k} \\
\vdots & \\
S_{i_{max}} & \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}
\end{array}
$$

Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in •

$$S_{i,k} := c(n) \text{ smallest elements of } \{0,1\}^n - M_{n,s}$$

Step s

S_0 | $\{\cdots\}$ $\uparrow$ $\{\cdots\}$

$\vdots$

S_i | $\{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}$ $S_{i,k}$

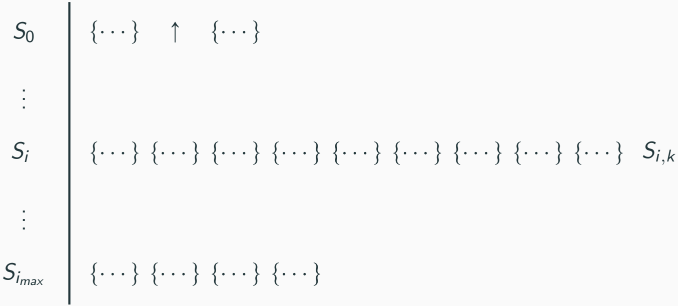
$\vdots$

$S_{i_{max}}$ | $\{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}$

Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in •

Step s



Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in • $\wedge\ n$ unlocked

For any j & x with $x \in E_s \wedge S_{j,x} \downarrow$ do: lock the n of $S_{j,x}$

Step s

$$
\begin{array}{c|l}
S_0 & \{\cdots\} \quad \uparrow \quad \{\cdots\} \\
\vdots & \\
S_i & \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\} \quad S_{i,k} \\
\vdots & \\
S_{i_{max}} & \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}
\end{array}
$$

Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in • $\wedge\ n$ unlocked

For any j & x with $x \in E_s \wedge S_{j,x} \downarrow$ do: lock the n of $S_{j,x}$ and force $S_{j,x} \subseteq \overline{R_\psi}$

Step ∞

$$
\begin{array}{c|l}
S_0 & \{\cdots\}\ \{\cdots\}\ \{\cdots\} \\
\vdots & \\
S_i & \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\} \\
\vdots & \\
S_{i_{max}} & \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}
\end{array}
$$

Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in • $\wedge$ n unlocked

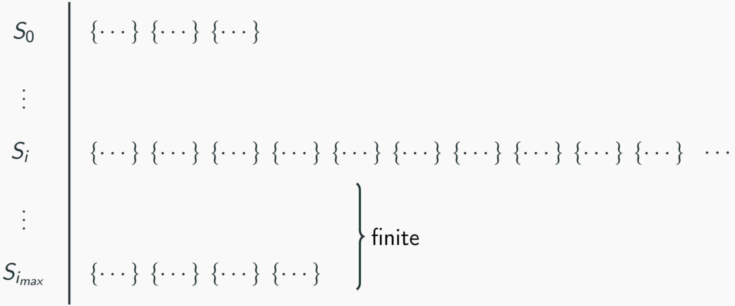
Step ∞

S_0	$\{\cdots\}\ \{\cdots\}\ \{\cdots\}$
$\vdots$	
S_i	$\{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \cdots$
$\vdots$	
$S_{i_{max}}$	$\{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}$

Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in • $\wedge\ n$ unlocked

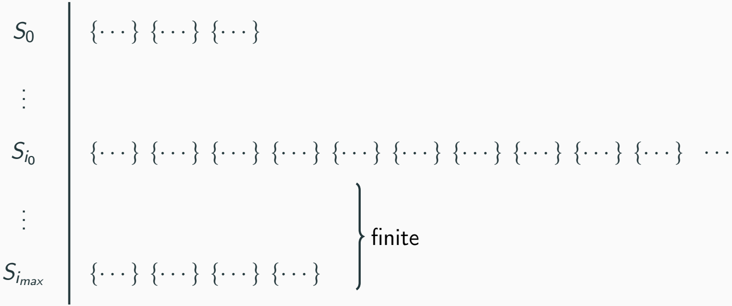
Step ∞



Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in • $\wedge$ n unlocked

Step ∞



Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in • $\wedge$ n unlocked

Step ∞

S_0 | $\{\cdots\}\ \{\cdots\}\ \{\cdots\}$

$\vdots$

S_{i_0} | $\{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \cdots$

$\vdots$

$S_{i_{max}}$ | $\{\cdots\}\ \{\cdots\}\ \{\cdots\}\ \{\cdots\}$

} finite

Choose greatest i ($\leqslant i_{max}$) and then smallest n ($\leqslant$ s) s.t.

$i * c(n) \leqslant |M_{n,s}| \wedge n$ not chosen in • $\wedge\ n$ unlocked

We now show $\exists x'.\forall x > x'.\ x \in E \Leftrightarrow S_{i_0,x} \subseteq \overline{R_\psi}$

Why does that work?

$$\exists x'.\forall x > x'.\ x \in E \Leftrightarrow S_{i_0,x} \subseteq \overline{R_\psi}$$

What is x'?

The least index s.t. after the definition of $S_{i_0,x'}$ no S_j $(j > i_0)$ gets extended

$\Rightarrow$: We know

- $\exists s.\ x \in E_s$
- $S_{i_0,x}$ is almost always defined

Reminder: The end of each step

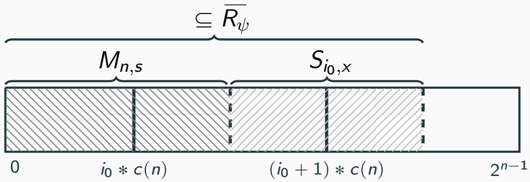
$\forall jx.\ x \in E_s \wedge S_{j,x} \downarrow$ do :

- force $S_{j,x} \subseteq \overline{R_\psi}$
- lock n

$$\Rightarrow S_{i_0,x} \subseteq \overline{R_\psi}$$

Why does that work?

$\Leftarrow$: We know $S_{i_0,x} \subseteq \overline{R_\psi}$



- $\exists s'.\ (i_0+1) * c(n) \leqslant |M_{n,s'}|$
- i_0 not greatest

unless n gets locked beforehand

$\Rightarrow x \in E$

Reminder:

- $S_{i_0,x} := c(n)$ smallest elements of $\{0,1\}^n - M_{n,s}$
- At the start of each step: Choose greatest i s.t.
  $i * c(n) \leqslant |M_{n,s}| \wedge n$ unlocked $\wedge \ldots$
- At the end of each step: $\forall jx.\ x \in E_s \wedge S_{j,x} \downarrow$ do :
  - force $S_{j,x} \subseteq \overline{R_\psi}$
  - lock n

The reduction: $E \leqslant_{tt} \overline{R_\psi}$

$$f : X \to \mathbb{LN} \times (\mathbb{LB} \to \mathbb{B})$$

$$f(x) = \begin{cases} (\varnothing, \lambda a.\text{true}) & x < x' \wedge x \in E \\ (\varnothing, \lambda a.\text{false}) & x < x' \wedge x \notin E \\ (S_{i_0,x}, \bigwedge) & x \geqslant x' \end{cases}$$

Conclusion

- The intricacies of Kummer's proof (not discussed here) make it hard to comprehend
- The proof idea is used in other related proofs
- The non-constructiveness will be a major challenge of the formalization

The road ahead:

- deciding on suitable definitions in Coq
- proving the results in the most straightforward way
- (beautifying as far as possible)

Thank you!

References

References

Kolmogorov, A. N. (1965).
Three approaches to the quantitative definition ofinformation'.
Problems of information transmission, 1(1):1–7.

Kummer, M. (1996).
On the complexity of random strings.
In Puech, C. and Reischuk, R., editors, *STACS 96*, pages 25–36. Springer Berlin Heidelberg.

Solomonoff, R. J. (1960).
A preliminary report on a general theory of inductive inference.
Citeseer.