The Kolmogorov-random numbers in synthetic computability theory

Nils Lauermann
Advisor: Fabian Kunze

Programming Systems Lab
Saarland University

August 26, 2021
• The Framework
• Simpleness of the Non-Random Numbers
  ⇒ Undecidability
  ⇒ Many-one Incompleteness
• Lower Bound for the count of Random Numbers
Constructive Type Theory: all functions $\mathbb{N} \to \mathbb{N}$ are computable

$\Rightarrow$ No external model of computation necessary

Instead we use a universal function $\phi$:

$\phi : \mathbb{N} \xrightarrow{\text{code}} \mathbb{N} \xrightarrow{\text{input}} \mathbb{N} \xrightarrow{\text{steps}} \mathbb{N} \cup \{\text{ON}\}$

$\phi$ is a partial function: Either $\phi$ always returns $\text{Some } x$ after some step count or diverges

\(^1\)Richman 1983; Bridges and Richman 1987; Bauer 2006.
\(^2\)Forster 2021.
All Coq functions are computable, so $\phi$ is universal for all (Coq) functions $\mathbb{N} \rightarrow \mathbb{N}$:

\[
\text{Church's Thesis}^3
\]

\[
\text{CT} := \forall f : \mathbb{N} \rightarrow \mathbb{N}. \exists c : \mathbb{N}. \forall x : \mathbb{N}. \exists s : \mathbb{N}. \phi^s_c x = \text{Some} \left( f \ x \right)
\]

There also exists a version of CT for partial (step-indexed) functions $f : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \mathbb{ON}$

---

$^3$Forster 2021.
To determine the size of a number we will use a bijective binary encoding:

- $\lceil \cdot \rceil : \mathbb{N} \rightarrow \text{LB}$
- $\lfloor \cdot \rfloor : \text{LB} \rightarrow \mathbb{N}$

with

- $\forall l : \text{LB}. \lfloor \lceil l \rceil \rfloor = l$
- $\forall n : \mathbb{N}. \lfloor \lceil n \rceil \rfloor = n$

For simplicity we assume this encoding.

Smullyan defines the 2-adic representation:\n
\[
\begin{array}{c|cccccccccccc}
   n & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots \\
\hline
   \lceil n \rceil & \epsilon & 0 & 1 & 00 & 01 & 10 & 11 & 000 & 001 & \cdots \\
\end{array}
\]

\[\text{Smullyan 2016.}\]
Kolmogorov Complexity\(^5\)

\[ \text{KC} : \quad \mathbb{N} \to \mathbb{N} \to \mathbb{N} \to \mathbb{P} \]

\[ \text{KC}_c \times k :\Leftrightarrow \text{least} (\lambda k. \exists is. |i| = k \land \phi^c_i = \text{Some } x) k \]

**Notation:** \( \text{KC}_c \times k \to p(k) \sim p(\text{KC}_c \times) \)

Reminder: Kolmogorov complexity is uncomputable

Universal Codes

Universal codes simulate any other code with linear overhead to the input size!

We have proven the existence of a universal code with CT for partial functions.

In the following $c$ will be a universal code.
The Random Numbers
The Random Numbers

More intuitive: incompressible numbers

**Definition: random numbers**

\[ R_c (x : \mathbb{N}) : \mathbb{P} := \forall is. \phi^i_n i = \text{Some } x \rightarrow |\lceil i \rceil| \geq |\lceil x \rceil| \]

In the literature: \( R_c x := KC_c x \geq |\lceil x \rceil| \)

**These definitions are classically equivalent:**
Decide termination of \( \phi \) with excluded middle.

---

\(^6\)Kolmogorov 1965.
The non-random numbers $\overline{R}_c$ are

- undecidable\(^7\)
- enumerable\(^7\)
- many-one incomplete\(^7\)
- truth-table complete\(^8\)

\(^7\)Zvonkin and Levin 1970.
\(^8\)Kummer 1996.
Definition: simple predicate

A predicate $p$ is simple if

- $p$ is enumerable
- $\overline{p}$ is infinite
- there is no infinite, enumerable sub-predicate of $\overline{p}$

Simple predicates are **undecidable** and **many-one incomplete**.

---

9 Post 1944.
10 Forster, Jahn, and Smolka 2021.
Non-Random Numbers: Enumerable

**Definition: enumerable predicate**¹¹

A predicate $p: X \rightarrow \mathbb{P}$ is enumerable if $\exists f: \mathbb{N} \rightarrow \mathbb{O}X. \forall x. px \leftrightarrow \exists n. fn = \text{Some } x$

Enumerator for $\overline{R}_c$:

$$\lambda \langle i, s \rangle. \text{ if } \phi^s_c i \text{ is Some } o$$

$$\text{ then if } i <_B o \text{ then Some } o \text{ else None}$$

$$\text{ else None}$$

¹¹Forster, Kirst, and Smolka 2019.
Random Numbers: Infinite

**Definition: infinite predicates**

A predicate \( p : X \rightarrow \mathbb{P} \) is infinite if
\[
\neg \exists l : \exists X. \forall x : X. px \rightarrow x \in l
\]

The random numbers are unbounded:

\[
\forall k. \neg \neg \exists x. |\lceil x \rceil| = k \land R_c x
\]

There are \( 2^k - 1 \) numbers \( i \) with \( |\lceil i \rceil| < k \) and \( 2^k \) numbers \( o \) with \( |\lceil o \rceil| = k \).

\[\Rightarrow\] There can be at most \( 2^k - 1 \) non-random numbers of length \( k \).

**Pigeonhole Principle:** There exists an \( x \) with \( |\lceil x \rceil| = k \) that must be random.

---

\(^{12}\)Forster, Jahn, and Smolka 2021.
**Definition: infinite predicates**

A predicate \( p : X \rightarrow \mathbb{P} \) is infinite if \( \neg \exists l : \mathbb{L}X. \forall x : X. px \rightarrow x \in l \).

---

**The random numbers are infinite:**

Given a list \( l \) that contains all random numbers.

By the unboundedness there exists a random number \( x \) with \( \lceil x \rceil = \max_{y \in l}(\lceil y \rceil + 1) \).

Contradiction!

\( \Rightarrow \) The random numbers must be infinite!

---

\(^{12}\)Forster, Jahn, and Smolka 2021.
Random Numbers: No infinite, enumerable sub-predicate

Reminder: Uncomputability of Kolmogorov complexity

Berry Paradox\textsuperscript{13}: The smallest number \(x\) with \(KC_c(x) > m\)

Almost identical proof:
The smallest number \(x\) that satisfies the sub-predicate and \(|\llbracket x \rrbracket| > m\).

Remark: Similarly to the uncomputability proof, Markov’s principle is used.

Assuming Markov’s principle, the non-random numbers are simple and hence undecidable and many-one incomplete!

\textsuperscript{13}Russell 1908.
Lower Bound for Random Numbers
A lower bound for the count of random numbers\textsuperscript{14}

Let $c$ be universal:
There exists a constant $d$ so that at least $\frac{1}{d}$ of the numbers of every length $k$ are random!

- Similar core idea as in Kummer’s truth-table completeness proof
- Currently uses excluded middle

\textsuperscript{14}Kummer 1996.
Conclusion
Conclusion

Working in synthetic computability is extremely natural and convenient!

Contributions

- To the best of our knowledge, the first formalization of Kolmogorov complexity
  - in Coq
  - in synthetic computability theory
- Undecidability of Kolmogorov complexity
- Simplicity of the non-random numbers
- Lower bound for the count of random numbers
- First steps towards a truth-table completeness proof of the non-random numbers in Coq
Related Work

Catt and Norrish formalized KC in HOL4:

- Classical logic
- With $\lambda$-calculus and general recursive functions as model of computation
- Focus on inequalities involving Kolmogorov complexity

Future Work

- Uncomputability/Simplicity: Investigate an elimination of Markov’s principle
- Truth-table completeness of the non-random numbers

Thank you!


<table>
<thead>
<tr>
<th>Content</th>
<th>Spec</th>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preliminaries</td>
<td>34</td>
<td>167</td>
</tr>
<tr>
<td>List Facts</td>
<td>78</td>
<td>557</td>
</tr>
<tr>
<td>Binary Encoding</td>
<td>65</td>
<td>453</td>
</tr>
<tr>
<td>Kolmogorov Complexity and Facts for KC</td>
<td>21</td>
<td>157</td>
</tr>
<tr>
<td>The Uncomputability of KC</td>
<td>14</td>
<td>162</td>
</tr>
<tr>
<td>Simplicity of the Non-Random Numbers</td>
<td>47</td>
<td>365</td>
</tr>
<tr>
<td>Lower Bound for the Random Numbers</td>
<td>64</td>
<td>838</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>323</td>
<td>2699</td>
</tr>
</tbody>
</table>
Lower Bound for Random Numbers
Reminder: Invariance Theorem\textsuperscript{15}

\[ \text{univ } c \rightarrow \forall c'. \exists d. \forall x. KC_c x \leq KC_{c'} x + d \]

\textbf{Goal}: Make a number \( x \), with \( \|\lceil x \rceil\| = k \), non-random with regard to \( c \):

\textbf{Idea}: Construct \( c' \) with \( KC_{c'} x < k - d \)

\textbf{Problem}: We cannot know \( d \) during the definition of \( c' \)

\textbf{Solution}: Incorporate \( d \) into input for \( c' \).

\textsuperscript{15}Kolmogorov 1965.
There exists a function $f : \mathbb{N} \rightarrow \mathbb{N}$ so that we can ensure the non-randomness of $2^{n-f(d)}$ numbers of length $n$.

### Which numbers will we force non-random?

For all $x < 2^{n-f(d)}$: Try to enumerate $2^n - x$ non-random numbers and make a number that was not enumerated random!

### There must be at least $2^{n-f(d)}$ random numbers of length $n$

Proof by Contradiction: Assume there are less than $2^{n-f(d)}$ random numbers. Then there are more than $2^n - 2^{n-f(d)}$ non-random numbers.

Some $x$ will enumerate all non-random numbers. Hence the number that is made non-random, is random. Contradiction!