RaNDomNess!

Verónica Becher

Universidad de Buenos Aires & CONICET

Global Perspectives on Reasoning and Scientific Method.
Workshop of the Division for Logic, Methodology, and Philosophy of Science and Technology. Salzburg, Austria.

November 30 and December 1, 2017.

Everyone has an intuitive idea about what is randomness, often associated with “gambling” or “luck”.

Azar - aléatoire - Zufall - rasgelelik - satunnaisuuden - slumpmässighet - randomness - aleatorietà

Everyone has an intuitive idea about what is randomness, often associated with "gambling" or "luck".

Today:

- Is there a mathematical definition of randomness?

Azar - aléatoire - Zufall - rasgelelik - satunnaisuuden - slumpmässighet - randomness - aleatorietà

Everyone has an intuitive idea about what is randomness, often associated with "gambling" or "luck".

Today:

- Is there a mathematical definition of randomness?
- Are there degrees of randomness?

Azar - aléatoire - Zufall - rasgelelik - satunnaisuuden - slumpmässighet - randomness - aleatorietà

Everyone has an intuitive idea about what is randomness, often associated with “gambling” or “luck”.

Today:

- Is there a mathematical definition of randomness?
- Are there degrees of randomness?
- Examples of randomness?

Azar - aléatoire - Zufall - rasgelelik - satunnaisuuden - slumpmässighet - randomness - aleatorietà

Everyone has an intuitive idea about what is randomness, often associated with “gambling” or “luck”.

Today:

- Is there a mathematical definition of randomness?
- Are there degrees of randomness?
- Examples of randomness?
- Can a computer produce a sequence that is truly random?

Everyone has an intuitive idea about what is randomness, often associated with “gambling” or “luck”.

Today:

- Is there a mathematical definition of randomness?
- Are there degrees of randomness?
- Examples of randomness?
- Can a computer produce a sequence that is truly random?
- Randomness ♥ Logic, Language and Information

Lady luck is fickle

Think of 0s and 1s.

A sequence is random if it can not be distinguished from independent tosses of a fair coin.

Lady luck is fickle

Would you believe that these have been obtained by independent tosses?

111111111111111111111111111111111111111111...

Lady luck is fickle

Would you believe that these have been obtained by independent tosses?

111111111111111111111111111111111111111111... ✗

Lady luck is fickle

Would you believe that these have been obtained by independent tosses?

111111111111111111111111111111111111111111... ✗

01001000100001000001000000100000001000000001...

Lady luck is fickle

Would you believe that these have been obtained by independent tosses?

111111111111111111111111111111111111111111... ✗

01001000100001000001000000100000001000000001... ✗

Lady luck is fickle

Would you believe that these have been obtained by independent tosses?

111111111111111111111111111111111111111111... ✗

01001000100001000001000000100000001000000001... ✗

100101010110001101110100010010101111001001..

Lady luck is fickle

Would you believe that these have been obtained by independent tosses?

111111111111111111111111111111111111111111... ✗
01001000100001000001000000100000001000000001... ✗
100101010110001101110100010010101111001001.. ✓

Heads and tails must occur with the same frequency.
Likewise for any combination of heads and tails.

Lady luck is fickle

Would you believe that these have been obtained by independent tosses?

111111111111111111111111111111111111111111... ✗

01001000100001000001000000100000001000000001... ✗

100101010110001101110100010010101111001001.. ✓

Heads and tails must occur with the same frequency.
Likewise for any combination of heads and tails.
¡Otherwise we would be able to guess it infinitely many times!

Randomness is impossibility to guess, to predict, to abbreviate....

Randomness is impossibility to guess, to predict, to abbreviate....

By whom?

By a human being?

Randomness is impossibility to guess, to predict, to abbreviate....

By whom?

By a human being? Ugh! we can not formalize it.

Randomness is impossibility to guess, to predict, to abbreviate....

By whom?

By a human being? Ugh! we can not formalize it.

By an automaton ?

Randomness is impossibility to guess, to predict, to abbreviate....

By whom?

By a human being? Ugh! we can not formalize it.

By an automaton ? Yes.

Randomness is impossibility to guess, to predict, to abbreviate....

By whom?

By a human being? Ugh! we can not formalize it.

By an automaton ? Yes. But there are different kinds...
Turing machines, pushdown automata, finite state automata.

Randomness is impossibility to guess, to predict, to abbreviate....

By whom?

By a human being? Ugh! we can not formalize it.

By an automaton ? Yes. But there are different kinds...
Turing machines, pushdown automata, finite state automata.

Turing machines yield the purest notion of randomness.

Randomness is impossibility to guess, to predict, to abbreviate....

By whom?

By a human being? Ugh! we can not formalize it.

By an automaton ? Yes. But there are different kinds...
Turing machines, pushdown automata, finite state automata.

Turing machines yield the purest notion of randomness.

Finite state automata yield the most basic notion of randomness .

Randomness is impossibility to guess, to predict, to abbreviate....

By whom?

By a human being? Ugh! we can not formalize it.

By an automaton ? Yes. But there are different kinds...
Turing machines, pushdown automata, finite state automata.

Turing machines yield the purest notion of randomness.

Finite state automata yield the most basic notion of randomness .

And there are intermediate notions.

A definition of randomness

A sequence is random for XXXX if, essentially, its initial segments can only be described explicitely

A definition of randomness

A sequence is random for XXXX if, essentially, its initial segments can only be described explicitely using an XXXX automaton.

A definition of randomness

A sequence is random for XXXX if, essentially, its initial segments can only be described explicitely using an XXXX automaton.

XXXX = Turing machines, Martin-Löf 1966; Chaitin 1975
XXXX = Finite-state automata, Borel 1909; Schnorr and Stimm 1971; Dai, Lathroup, Lutz and Mayordomo 2005

A definition of randomness

A sequence is random for XXXX if, essentially, its initial segments can only be described explicitely using an XXXX automaton.

XXXX = Turing machines, Martin-Löf 1966; Chaitin 1975
XXXX = Finite-state automata, Borel 1909; Schnorr and Stimm 1971; Dai, Lathroup, Lutz and Mayordomo 2005

Randomness for Turing machines (pure randomness)

Randomness for Turing machines (pure randomness)

A sequence is random for Turing machines if, essentially, its initial segments can only be described explicitely

Randomness for Turing machines (pure randomness)

A sequence is random for Turing machines if, essentially, its initial segments can only be described explicitly using a Turing machine . That is, its initial segments cannot be compressed with a Turing machine.

Randomness for Turing machines (pure randomness)

A sequence is random for Turing machines if, essentially, its initial segments can only be described explicitly using a Turing machine . That is, its initial segments cannot be compressed with a Turing machine.

Formally, a sequence is random if its initial segments have almost maximal descriptive complexity .

Descriptive / Kolmogorov / program-size complexity

Some long strings can be described using fewer symbols than their length; this is used in data compression .

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

For example, a string consisting of 2^n many a's can be encoded as $\log n$ many symbols plus a constant:

$$\texttt{input } n\texttt{; i=0; while (i<}2^n\texttt{) \{print } a\texttt{; i=i+1;\}}$$

Descriptive / Kolmogorov / program-size complexity

Definition (Chaitin 1975)

Fix a universal Turing machine U with prefix-free domain .
The descriptive of a string s, $K(s)$, is the length of the shortest input in U that outputs s.

For every string s, $K(s) \leq |s| + 2\log|s| + constant$.

The definition of randomness

Definition (Chaitin 1975)

A sequence $a_1a_2a_3\ldots$ is random if $\exists c\ \forall n\ K(a_1a_2\ldots a_n) > n - c$.

How do we know that the definition is right?

How do we know that the definition is right?

The definition of randomness was accepted when two different formulations were shown to be equivalent.

This is similar to what happenned with the notion of algorithm in 1930s with Church-Turing thesis.

An equivalent definition of randomness

Definition (Martin-Löf 1965, tests of non-randomness)

A sequence is Martin-Löf random if it passes all computably definable tests of non-randomness.

An equivalent definition of randomness

Definition (Martin-Löf 1965, tests of non-randomness)

A sequence is Martin-Löf random if it passes all computably definable tests of non-randomness.

Technically, a sequence is Martin-Löf random if it belongs to no computably definable null set.

An equivalent definition of randomness

Definition (Martin-Löf 1965, tests of non-randomness)

A sequence is Martin-Löf random if it passes all computably definable tests of non-randomness.

Technically, a sequence is Martin-Löf random if it belongs to no computably definable null set.

Theorem (Schnorr 1975)

Chaitin's and Martin-Löf's definitionare equivalent.

Examples of random sequences

Examples of random sequences

Have you ever experienced that your computer locked up (froze)?

Examples of random sequences

Have you ever experienced that your computer locked up (froze)?

Ω-numbers

Theorem (Chaitin 1975)

The probability that a universal Turing machine with prefix-free domain halts, is random.

Ω-numbers

Theorem (Chaitin 1975)

The probability that a universal Turing machine with prefix-free domain halts, is random.

$$\Omega = \sum_{U(p)\textit{halts}} 2^{-|p|},$$

Ω-numbers

Theorem (Chaitin 1975)

The probability that a universal Turing machine with prefix-free domain halts, is random.

$$\Omega = \sum_{U(p)\, \textit{halts}} 2^{-|p|},$$

Ω numbers: probabilities of other computer behaviours

(Becher,Chaitin 2001,2003; Becher,Grigorieff 2005,2009: Becher, Figueira, Grigorieff, Miller 2006; Barmpalias 2016)

Randomness ♥ Logic

Randomness ♥ Logic

The Berry's paradox

Randomness ♥ Logic

The Berry's paradox

Give the smallest positive integer not definable in fewer than thirteen words.

Randomness ♥ Logic

The Berry's paradox

Give the smallest positive integer not definable in fewer than thirteen words.

The above sentence has twelve.

Randomness ♥ Logic

The Berry's paradox

Give the smallest positive integer not definable in fewer than thirteen words.

The above sentence has twelve.

G.G.Berry 1867–1928, librarian at Oxford's Bodleian library.

G.Boolos (1989) built on a formalized version of Berry's paradox to prove Gödel's Incompleteness Theorem formalizing the expression "m is the first number not definable in less than k symbols".

X.Caicedo (1993), La paradoja de Berry revisitada, o la indefinibilidad de la definibilidad y las limitaciones de los formalismos Lecturas Matemáticas 14: 37-48.

Berry's paradox

Though the formal analogue does not lead to a logical contradiction, it yields a proof that descriptive complexity K is not computable.

Questions and answers about random sequences

Are almost all sequences random?

Questions and answers about random sequences

Are almost all sequences random?

Yes. By Martin Löf's definition, the set of random sequences is the whole set minus the effectively defined universal null set. Then, with probability 1 an arbitrary sequence belongs to the set of random sequences.

Questions and answers about random sequences

Is there a hierarchy of randomness?

Questions and answers about random sequences

Is there a hierarchy of randomness?

Yes. there is a hierarchy of automata. For example, incompressibility by Turing machines imples incompressibility by finite automata.

Questions and answers about random sequences

Is the spell of good luck (or bad luck) necessarily short?

Questions and answers about random sequences

Is the spell of good luck (or bad luck) necessarily short?

Yes ("Nothing lasts forever. . . ").

Proof: Think of 0s and 1s. Suppose a random sequence starts $a_1 a_2 ... a_n$. If there is a run of 0's longer than $\log n$, then $a_1 a_2 ... a_n$ is compressible. Randomness ensures that this will happen only finitely many times.

Questions and answers about random sequences

Can a computer output a random sequence?

Questions and answers about random sequences

Can a computer output a random sequence?

"Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin."

John Von Neumann (1951). Various techniques used in connection with random digits.

Questions and answers about random sequences

Can a computer output a random sequence?

"Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin."

John Von Neumann (1951). Various techniques used in connection with random digits.

Proof: Every computable sequences is dramatically compressible by a Turing machine! An initial segment of length n can be compressed to $2\log n+$constant. Hence, computable sequences are not random.

Randomness ☠ Computers

Random number generators (pseudo randomness)
USA National Institute of Standards and Technology
`http://csrc.nist.gov/groups/ST/toolkit/rng/`

Randomness ☠ Computers

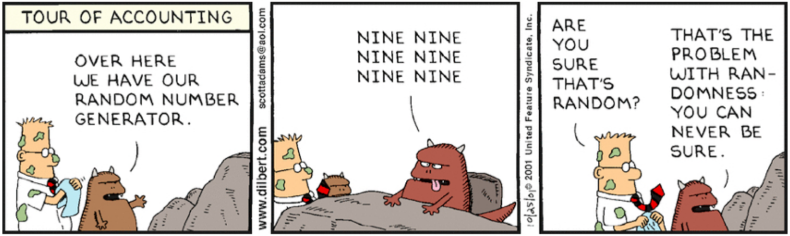
Random number generators (pseudo randomness)
USA National Institute of Standards and Technology
`http://csrc.nist.gov/groups/ST/toolkit/rng/`

`http://www.random.org/`

Randomness ☠ Computers

Random number generators (pseudo randomness)
USA National Institute of Standards and Technology
`http://csrc.nist.gov/groups/ST/toolkit/rng/`

`http://www.random.org/`



Randomness ♥ Information

Randomness ♥ Information

Descriptive Theory

Randomness ♥ Information

Definition (Shannon 1948)

Given a probability P of a discrete random variable X, the entropy
$H(X) = \sum_x P(x = X)(-\log P(x = X)))$.

Definition (Chaitin 1975)

Given a universal Turing U machine with prefix-free domain.
$K(s) = \min\{|t| : U(t) = s\}$, $P(s) = \sum_{t:U(t)=s} 2^{-|t|}$.

Theorem (Chaitin 1975)

For every string s, $K(s) \simeq \lceil -\log P(s) \rceil$.

Shannon's entropy is formally equal to expected descriptive complexity:

$$\sum_s P(s)(-\log P(s)) \simeq \sum_s P(s)K(s).$$

Randomness ♥ Language

Randomness ♥ Language

A sequence is random (relative to some computing power) if, essentially, the only way to describe it is explicitely.

Randomness ♥ Language

A sequence is random (relative to some computing power) if, essentially, the only way to describe it is explicitely.

Therefore, randomness of a given sequence is about how we can describe its initial segments in the language , according to the computing power.

Randomness ♥ Language

A sequence is random (relative to some computing power) if, essentially, the only way to describe it is explicitely.

Therefore, randomness of a given sequence is about how we can describe its initial segments in the language , according to the computing power.

Thus, randomness is a matter of language.

Randomness ♥ Language

A sequence is random (relative to some computing power) if, essentially, the only way to describe it is explicitely.

Therefore, randomness of a given sequence is about how we can describe its initial segments in the language , according to the computing power.

Thus, randomness is a matter of language.

The End