SIGMA camp 20/08/2020

# what is randomness?

alexander.shen@lirmm.fr, www.lirmm.fr/~ashen

LIRMM CNRS & University of Montpellier

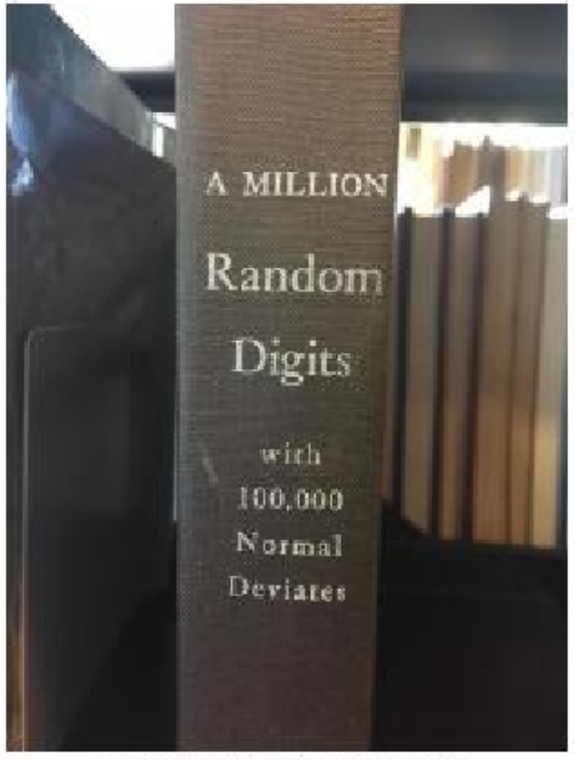
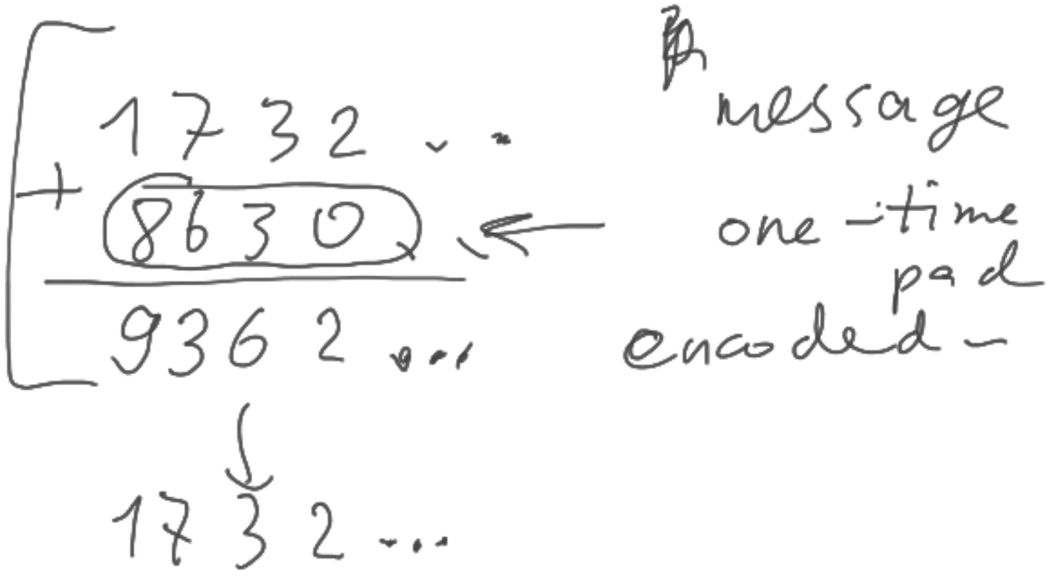



TABLE OF RANDOM DIGITS

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 00050 | 09188 | 20097 | 32825 | 39527 | 04220 | 86304 | 83389 | 87374 | 64278 | 58044 |
| 00051 | 90045 | 85497 | 51981 | 50654 | 94938 | 81997 | 91870 | 76150 | 68476 | 64659 |
| 00052 | 73189 | 50207 | 47677 | 26269 | 62290 | 64464 | 27124 | 67018 | 41361 | 82760 |
| 00053 | 75768 | 76490 | 20971 | 87749 | 90429 | 12272 | 95375 | 05871 | 93823 | 43178 |
| 00054 | 54016 | 44056 | 66281 | 31003 | 00682 | 27398 | 20714 | 53295 | 07706 | 17813 |

# Why would you need this book?

1. Cryptography

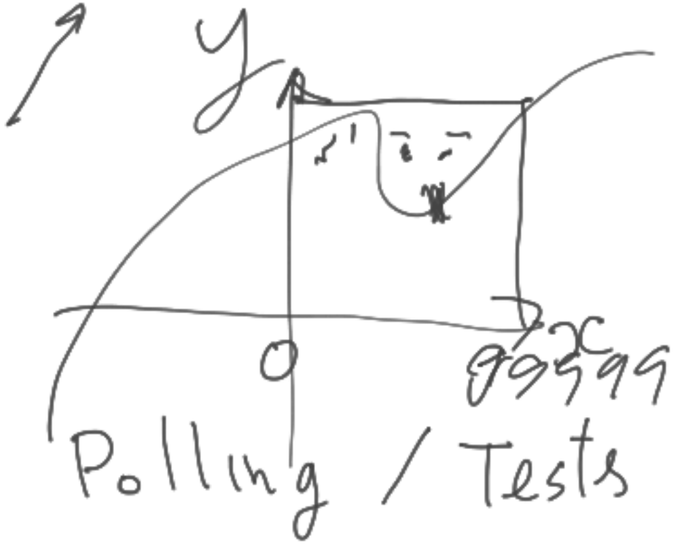



2. Find a random number for testing some claim

3. Randomized algorithms

$$(x^2+y^2)^2-(2xy)^2=(x^2-y^2)^2$$

$x=0$ $y=0$ +



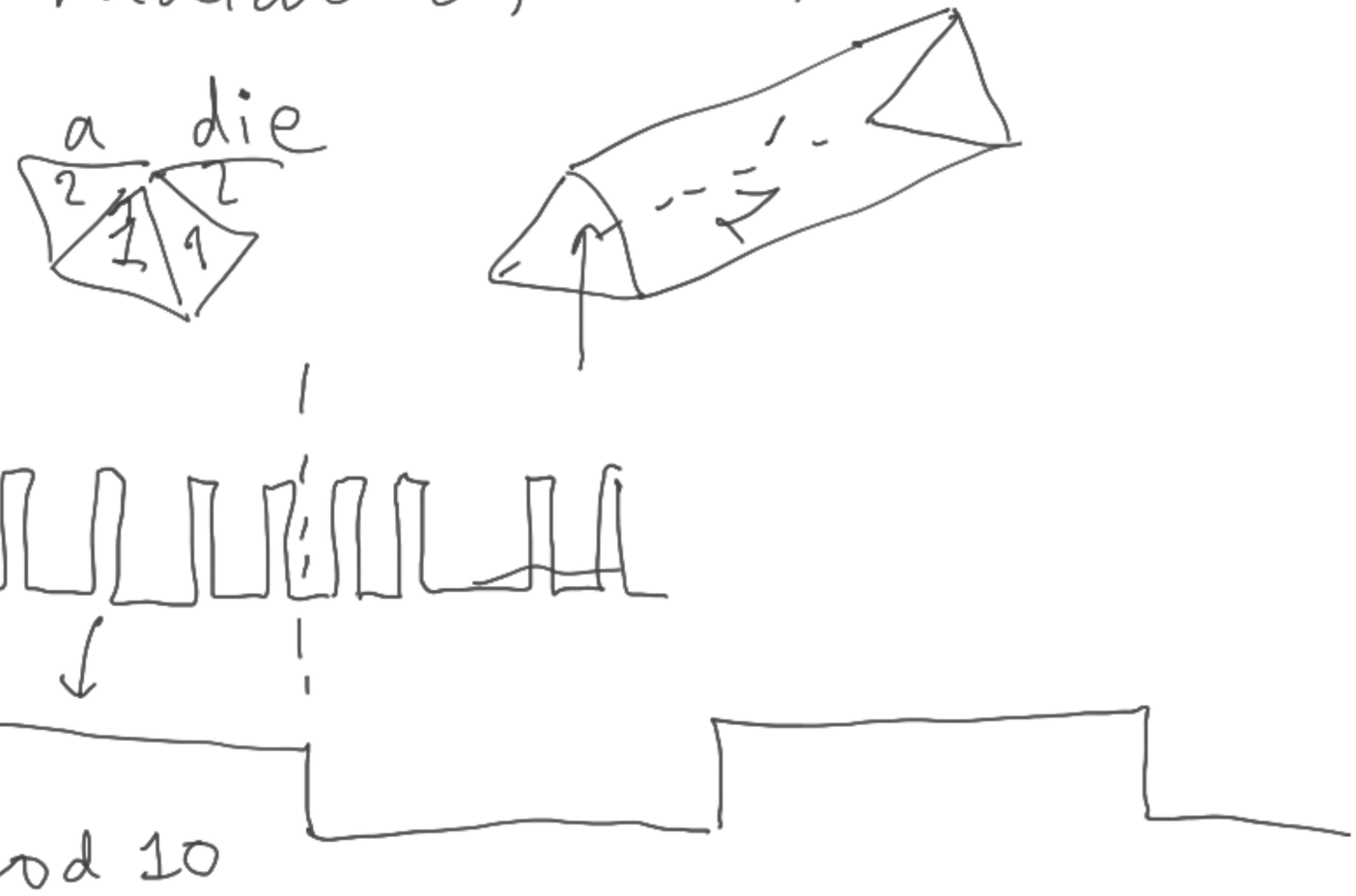

4. Polling / Tests

01 02 ... 09

+ medicine ↓ | - placebo ↓

# How can you produce such a book?

1. Use some natural phenomena
   radiation, noise, radiowaves
2. Roll a die

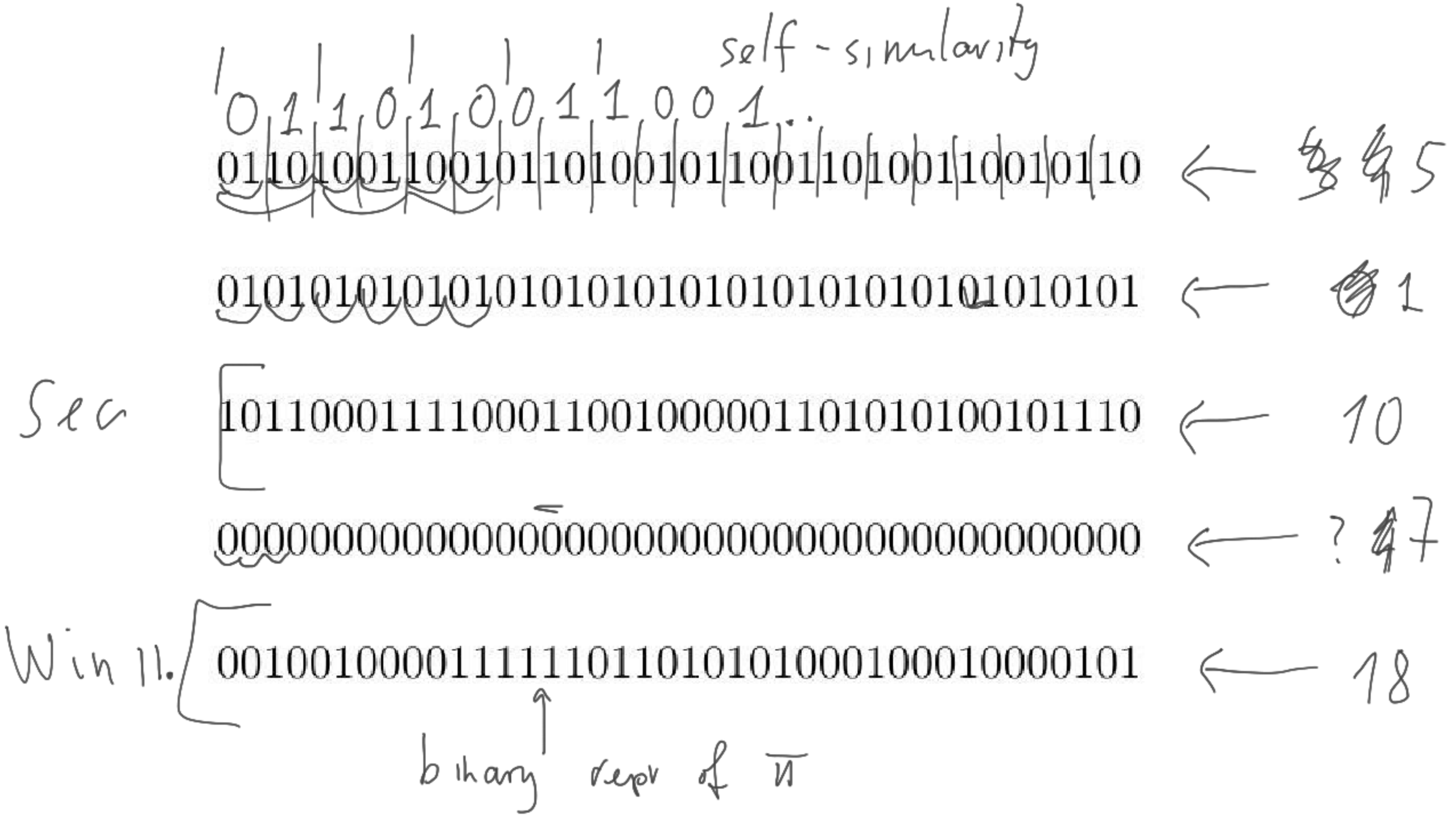


# Quality control?

When a sequence of bits can be called random?

A historical fact or a property of a sequence?

If a property, which one? How can we (dis)prove it?


self-similarity
0 1 1 0 1 0 0 1 1 0 0 1 ...
01101001100101101001011001101001011001101001011010
01010101010101010101010101010101010101010101010101
Sec
10110001111000110010000011010101001011101
00000000000000000000000000000000000000000000000000
Win 11.
00100100001111111011010101000100010000101
binary repr of π
← 5
← 1
← 10
← ? 47
← 18

~1965

A binary string is "random" if there is no shorter program that produces this string

print("0110111 ...")

Shorter than what?

for i in range(1000000) print('01', end='')

Complexity of $x$: minimal length of a program that produces $x$. (Notation: $C(x)$)

Programming language?

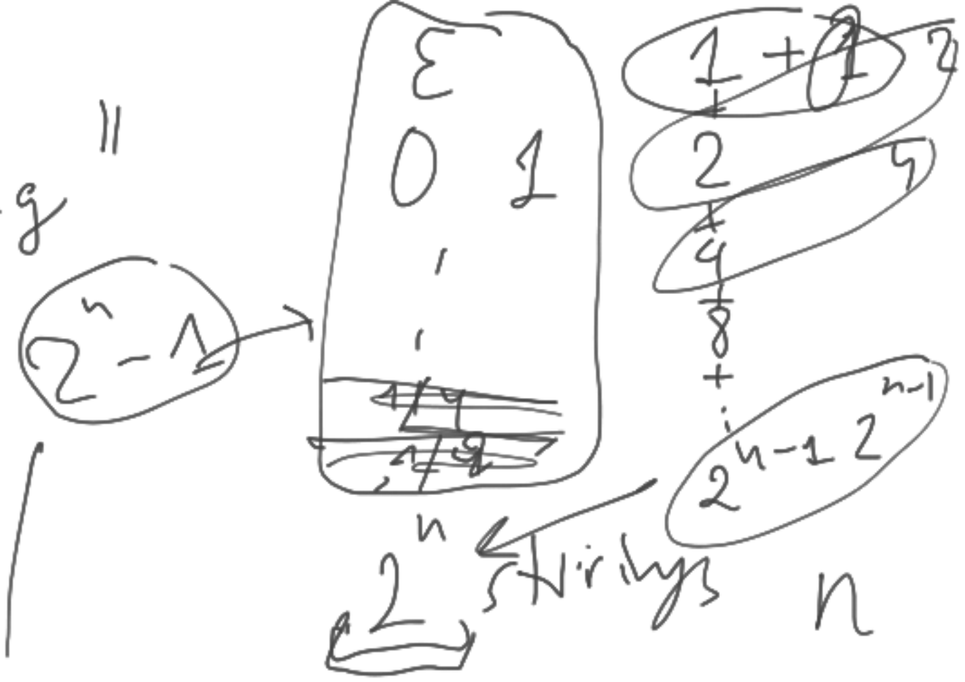
Not important

Fix

Randomness = incompressibility. Do incompressible strings exist?

(python int  python pr) C program

"Random = incompressing"




What is a probability of getting a random string by tossing a coin?

„Every string is compressible"

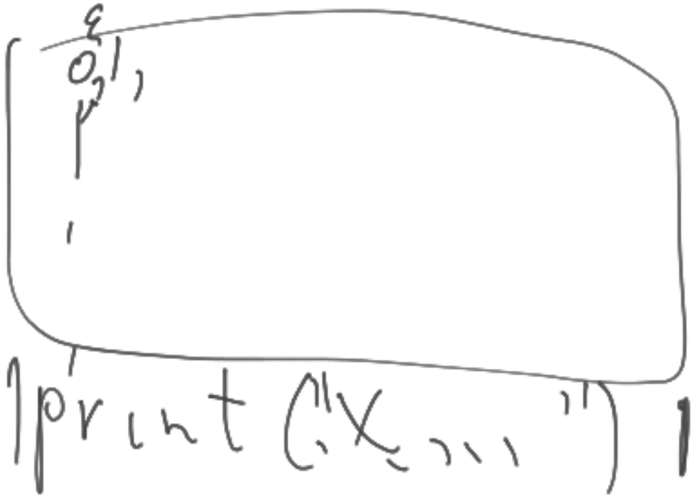
$n \longrightarrow n-1 \longrightarrow n-2 \longrightarrow$ '0'

n-bit string $2^n$ | shorter program $< n$

A string is given. Can we find whether it is random? is there a program that computes its complexity?

(Theoretically. No time restrictions.)

Why not to try all short programs?




Shorter programs

Given: ~~X~~

Find: length of the short. program prod. X

The minimal positive integer that cannot be uniquely defined by less that billion English words

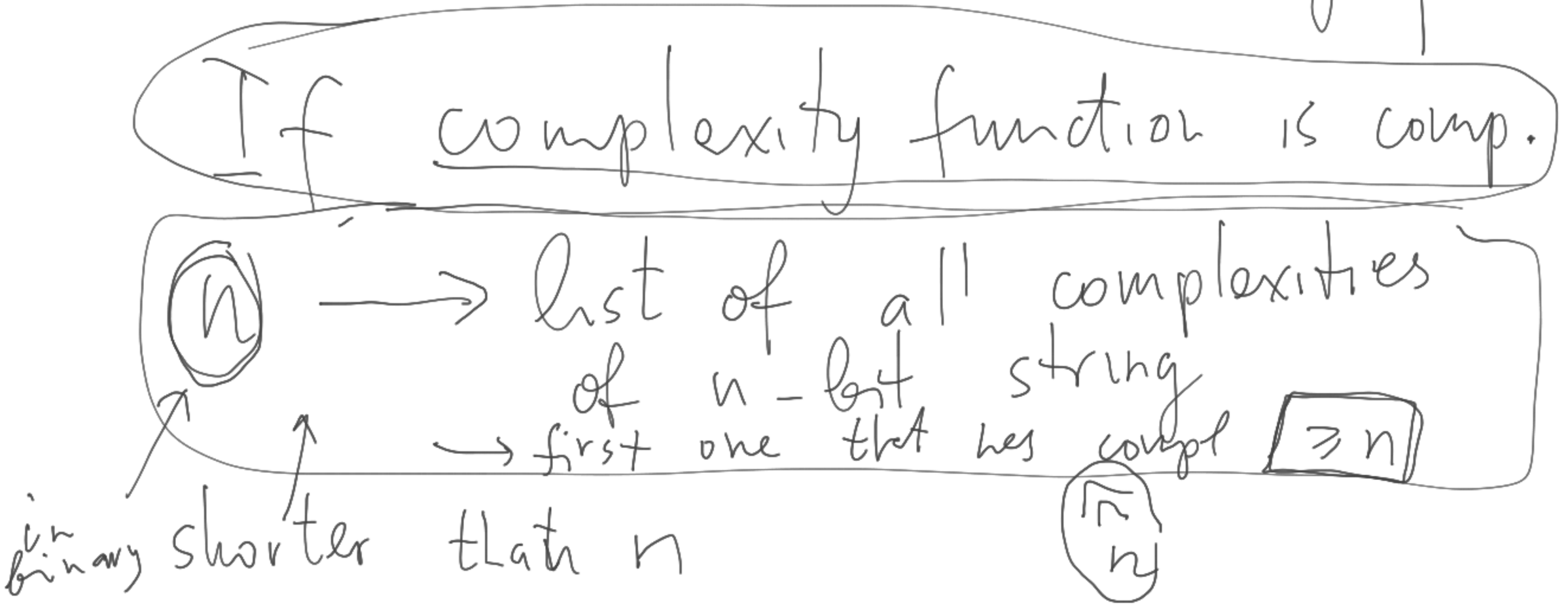
Berry paradox

The minimal $n$-bit string that has complexity at least $n$

complexity at least $n$ or $\log n$ plus constant?

Halt. problem undecidable

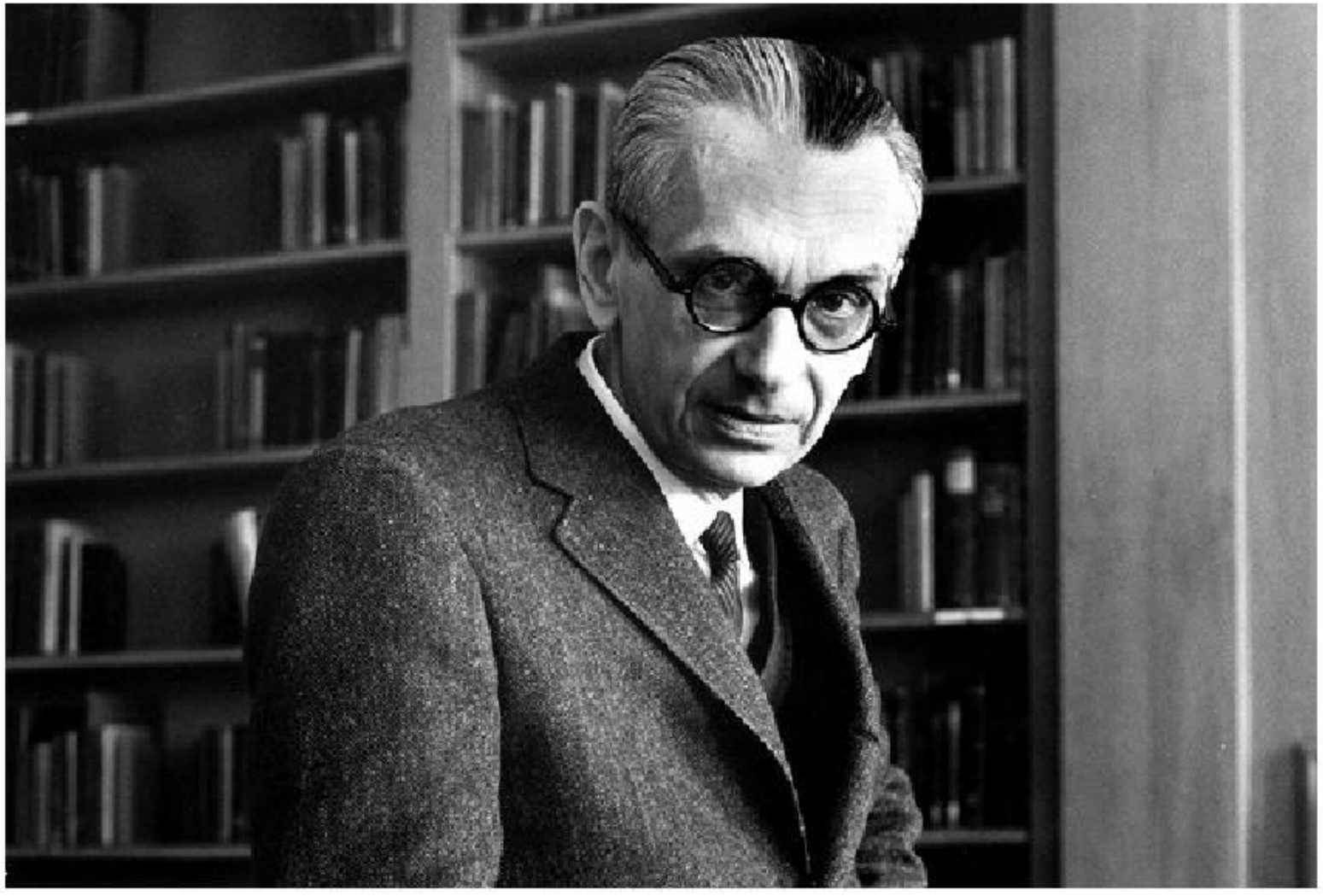
$n$ large ↑



Theorem: Complexity function is not computable.

Not all mathematical truths can be proven (assuming machine-checkable proof).

First $n$ bit string that is provably of compl $\geq n$



1 2 3 4 5 . . 10 11 12 13 . .

[1978 Helsinki]