# What is Complexity? 

Notes for CAS, 28-4-2020
Loe Feijs


## What is complexity and how to measure complexity?

- Computational complexity
$\checkmark$ practice: example in Processing
$\checkmark$ theory: big-O notation
$\checkmark$ theory: NP-complete problems
- Information theory complexity
$\checkmark$ Shannon's aproach:
$\checkmark$ Kolmogorov's approach:


P naive | Processing 2.2.1
File Edit Sketch Tools Help


Done Saving.
//fibonacci numbers using recursion
//Loe Feijs and TU/e for CAS 2020
long fibonacci(long n)\{
if ( $\mathrm{n}<=1$ )
return 1;
input, output, time: 1, 1, 0
input, output, time: 2, 2, 0
input, output, time: 3, 3, 0
input, output, time: 4, 5, 0
input, output, time: 5, 8, 0
input, output, time: 6, 13, 0
input, output, time: 7, 21, 0
input, output, time: 8, 34, 0
input, output, time: 9, 55, 0
input, output, time: 10, 89, 0
input, output, time: 11, 144, 0
input, output, time: 12, 233, 0
input, output, time: 13, 377, 0
input, output, time: 14, 610, 0
input, output, time: 15, 987, 0
input, output, time: 16, 1597, 0
input, output, time: 17, 2584, 0
input, output, time: 18, 4181, 0
input, output, time: 19, 6765, 0
input, output, time: 20, 10946, 0
input, output, time: 21, 17711, 0
input, output, time: 22, 28657, 0
input, output, time: 23, 46368, 0
//fibonacci numbers using recursion
//Loe Feijs and TU/e for CAS 2020
long fibonacci(long n) \{

$$
\text { if }(\mathrm{n}<=1)
$$

return 1;

## input, output, time: 26, 196418, 0

input, output, time: 27, 317811, 1
input, output, time: 28, 514229, 1
input, output, time: 29, 832040, 2
input, output, time: 30, 1346269, 3
input, output, time: 31, 2178309, 5
input, output, time: 32, 3524578, 9
input, output, time: 33, 5702887, 15
input, output, time: 34, 9227465, 24
input, output, time: 35, 14930352, 41
input, output, time: 36, 24157817, 60
input, output, time: 37, 39088169, 98
input, output, time: 38, 63245986, 166
input, output, time: 39, 102334155, 262
input, output, time: 40, 165580141, 436
input, output, time: 41, 267914296, 682
input, output, time: 42, 433494437, 1164
input, output, time: 43, 701408733, 1882
input, output, time: 44, 1134903170, 3043
input, output, time: 45, 1836311903, 4778
input, output, time: 46, 2971215073, 7936
input, output, time: 47, 4807526976, 12856


P smart | Processing 2.2.1
//fibonacci numbers using memoization
//Loe Feijs and TU/e for CAS 2020
long fibonacci(int n)\{
if (memo[n] > 0)
return memo[n];
else if ( $n<=1$ )
return 1;
else return memo[n] = fibonacci(n - 1) + fibonacci(n - 2);
\}
int n ;
long t ;
long[] memo;
void setup()\{
$\mathrm{n}=0 ;$
memo = new long[100];
for (int $\mathbf{i}=0 ; \mathbf{i}<100 ; i++$ )
memo[i] $=0$;
\}
void draw() \{
if ( n < 47) \{
n++;
$\mathrm{t}=$ System. currentTimeMillis();
long fibo = fibonacci(n);
long time $=$ System. currentTimeMillis() - t;
println("input, output, time: " + n + ", " + fibo + ", " + time);
\}
\}

```
fibonacci numbers using memoization
//Loe Feijs and TU/e for CAS 2020
long fibonacci(int n){
    if (memo[n] > 0)
        return memo[n];
```

input, output, time: 1, 1, 0
input, output, time: 2, 2, 0
input, output, time: 3, 3, 0
input, output, time: 4, 5, 0
input, output, time: 5, 8, 0
input, output, time: 6, 13, 0
input, output, time: 7, 21, 0
input, output, time: 8, 34, 0
input, output, time: 9, 55, 0
input, output, time: 10, 89, 0
input, output, time: 11, 144, 0
input, output, time: 12, 233, 0
input, output, time: 13, 377, 0
input, output, time: 14, 610, 0
input, output, time: 15, 987, 0
input, output, time: 16, 1597, 0
input, output, time: 17, 2584, 0
input, output, time: 18, 4181, 0
input, output, time: 19, 6765, 0
input, output, time: 20, 10946, 0
input, output, time: 21, 17711, 0
input, output, time: 22, 28657, 0
input, output, time: 23, 46368, 0

P smart | Processing 2.2.1
//fibonacci numbers using memoization
//Loe Feijs and TU/e for CAS 2020
long fibonacci(int n)\{
if (memo[n] > 0)
return memo[n];

Done Saving.
input, output, time: 23, 46368, 0
input, output, time: 24, 75025, 0
input, output, time: 25, 121393, 0
input, output, time: 26, 196418, 0
input, output, time: 27, 317811, 0
input, output, time: 28, 514229, 0
input, output, time: 29, 832040, 0
input, output, time: 30, 1346269, 0
input, output, time: 31, 2178309, 0
input, output, time: 32, 3524578, 0
input, output, time: 33, 5702887, 0
input, output, time: 34, 9227465, 0
input, output, time: 35, 14930352, 0
input, output, time: 36, 24157817, 0
input, output, time: 37, 39088169, 0
input, output, time: 38, 63245986, 0
input, output, time: 39, 102334155, 0
input, output, time: 40, 165580141, 0
input, output, time: 41, 267914296, 0
input, output, time: 42, 433494437, 0
input, output, time: 43, 701408733, 0
input, output, time: 44, 1134903170, 0
input, output, time: 45, 1836311903, 0
input, output, time: 46, 2971215073, 0
input, output, time: 47, 4807526976, 0

## Theory: Big-O notation

- Two programs:
$\checkmark$ naive.pde (compute the $\mathrm{n}^{\text {th }}$ Fibonacci number)
$\checkmark$ smart.pde (idem)
- Big-O notation characterizes a function according to its growth rate $\checkmark$ write $T_{1}(n)$ for the execution time of the first program, given $n$
- $\mathrm{T}_{1}(\mathrm{n})=O\left(2^{\mathrm{n}}\right)$
$\checkmark$ meaning that for sufficiently large $n$ $\mathrm{T}_{1}(\mathrm{n})$ does not grow faster than $2^{\mathrm{n}}$
$\checkmark$ formally: there exist constants C and N such that $T_{1}(n) \leq C \times 2^{n}$ for all $n>N$

Recommended reading: http://web.mit.edu/16.070/ www/lecture/big_o.pdf

Fact: $\mathrm{T}_{1}(\mathrm{n})=O\left(2^{\mathrm{n}}\right)$
Stronger statement: $\mathrm{T}_{1}(\mathrm{n})=O\left(1.63^{\mathrm{n}}\right)$

What about the second program?
Fact: $\mathrm{T}_{2}(\mathrm{n})=O(\mathrm{n})$
which is a significant improvement

Typical complexities:

| $O(1)$ | constant |
| :--- | :--- |
| $O(\mathrm{n})$ | linear |
| $O\left(\mathrm{n}^{2}\right)$ | quadratic |
| $O\left(\mathrm{n}^{\mathrm{c}}\right)$ | polynomial |
| $O\left(\mathrm{c}^{\mathrm{n}}\right)$ | exponential |

Recommended reading: http://web.mit.edu/16.07
0/www/lecture/big_o.pdf

## NP-complete problems

- A problem is a well-defined program specification
$\checkmark$ compute the $n^{\text {th }}$ Fibonacci number
$\checkmark$ sort any given list of $n$ numbers
$\checkmark$ find a shortest path from a to b in any network of $n$ nodes (distances given)
$\checkmark$ find a shortest return path along all $n$ nodes in a network (distances given)


The last problem is called the "Travelling Salesman Problem" Theory:
it belongs to the class of NP-complete problems
for which any solution program's execution time is $O\left(\mathrm{c}^{n}\right)$
whether polynomial solution programs exist is an open problem
solving this " $\mathrm{P}=\mathrm{NP}$ " problem deserves a $\$ 1,000,000$ Millenium-prize Practice:
find good-enough approximations, not shortest these problems pop-up in design, e.g. our WS lab
 Maven, Styling: Giorgia Presti, Photos wire.net/pied-de-pulse/


## Computational complexity: an overview

- Each program has a run-time complexity
$\checkmark$ naive fibonacci: exponential
$\checkmark$ smart Fibonacci: linear
- Each problem belongs to a complexity class, for example:
$\checkmark$ problems having polynomial solutions (e.g. Fibonacci)
$\checkmark$ problems having exponential solutions, no polynomial (if $\mathrm{P} \neq \mathrm{NP}$ )
$\checkmark$ problems having no solutions at all (e.g. the halting problem)


# Information entropy as a measure for complexity 

Notes for CAS<br>Feijs, 2019-2020



How to measure complexity?

- Shannon's aproach: assume a source which produces random messages, how many bits do we need on average to code a message?

```
A Mathematical Theory of Communication", Bell System Technical
Journal, vol. 27, pp. 379-423 & 623-656, 1948
```

- Kolmogorov's approach: assume a fixed message (a tekst, or an image, for example), how long is the shortest program that will reproduce the message?

```
Kolmogorov, A. (1968). Logical basis for information theory and
probability theory. IEEE Transactions on Information Theory,
14(5), 662-664.
```



Andrei Kolmogorov Source: http://www.mi.ras.ru

## Examples:

- "010011010110100110010011100101001001011001"
- "0000000000000010000000000000100000000000001"
- int tm(int i, int N)\{int im = i\%(2*N); return im<N? im : (2*N)-im;\}
- "a[i][j] $=(\operatorname{tm}(\mathrm{i}, \mathrm{N})+1000+1-\operatorname{tm}(\mathrm{j}-1, \mathrm{~N}+1)) \% 4<2$ ? true : false;"
- 



Shannon's aproach:
Assume source $X$
with alphabet $\{A, B, C, D\}$
and probabilities $P(A)=0.5, P(B)=0.25, P(C)=0.125, P(D)=0.125$
Information per letter
$H(A)=-{ }^{2} \log 0.5=-(-1)=1$ bit
$H(B)=-{ }^{2} \log 0.25=-(-2)=2$ bit
$H(C)=-{ }^{2} \log 0.125=-(-3)=3$ bit
$H(D)=-{ }^{2} \log 0.125=-(-3)=3$ bit
Complexity of this source
$H(X)=1 / 2.1+1 / 4.2+1 / 8 \cdot 3+1 / 8 \cdot 3=13 / 4=1.75$ bit per letter

Shannon's aproach:
Claim: we can code these letters in 1.75 bit (on average)
"Huffman coding"
$\mathrm{A} \rightarrow 0$
B $\rightarrow 10$
C $\rightarrow 110$
D $\rightarrow 111$

Decoding: BABADACA was 10010011101100 DDDDDDD was 11111111111111111111111

$$
H(X)=\sum_{i}-p_{i}{ }^{2} \log p_{i}
$$

## Special case:

two-letter alphabet

$$
\begin{aligned}
& P(A)=p_{1}=p \\
& P(B)=p_{2}=(1-p)
\end{aligned}
$$

$$
H(X)=-p^{2} \log p-(1-p)^{2} \log (1-p)
$$



Fig. 7 -Entropy in the case of two possibilities with probabilities $p$ and $(1-p)$.
Source: A Mathematical Theory of Communication", Bell System Technical Journal, vol. 27, pp. 379-423 \& 623-656, 1948

## III. The Series of Approximations to English

To give a visual idea of how this series of processes approaches a language, typical sequences in the approximations to English have been constructed and are given below. In all cases we have assumed a 27 -symbol "alphabet," the 26 letters and a space.

1. Zero-order approximation (symbols independent and equiprobable).

XFOML RXKHRJFFJUJ ZLPWCFWKCYJ FFJEYVKCQSGHYD QPAAMKBZAACIBZLHJQD.
2. First-order approximation (symbols independent but with frequencies of English text).

OCRO HLI RGWR NMIELWIS EU LL NBNESEBYA TH EEI ALHENHTTPA OOBTTVA NAH BRL.
3. Second-order approximation (digram structure as in English).

ON IE ANTSOUTINYS ARE T INCTORE ST BE S DEAMY ACHIN D ILONASIVE TUCOOWE AT TEASONARE FUSO TIZIN ANDY TOBE SEACE CTISBE.
4. Third-order approximation (trigram structure as in English).

IN NO IST LAT WHEY CRATICT FROURE BIRS GROCID PONDENOME OF DEMONSTURES
OF THE REPTAGIN IS REGOACTIONA OF CRE. Source: A Mathematical Theory of Communication", Bell System
Later, (1951, Shannon): English between .5 and 1.3 bit per char

How to measure complexity, $2^{\text {nd }}$ approach?

- Kolmogorov's approach: assume a fixed message
(a tekst, or an image, for example), how long is the shortest program that will reproduce the message?

```
Kolmogorov, A. (1968). Logical basis for information theory and
probability theory. IEEE Transactions on Information Theory,
14(5), 662-664.
```



Andrei Kolmogorov
Source: http://www.mi.ras.ru

# Logical Basis for Information Theory and Probability Theory 

ANDREI N. KOLMOGOROV

Abstract-A new logical basis for information theory as well as probability theory is proposed, based on computing complexity.

## Section I

WYE SHALL be concerned with the main basic concepts of information theory, beginning with the traditional concept of the conditional entropy of $x$ when the value of $y$ is known, $H(x \mid y)$, which can be interpreted as the quantity of information required for computing ("programming") the value $x$ when the value $y$ is already known. By using $\phi$ to denote a particular given known value, we get the unconditional entropy

$$
H(x \mid \phi)=H(x)
$$

Information given by $y$ concerning the value of $x$ can, as is well known, be expressed:

$$
I(x \mid y)=H(x)-H(x \mid y)
$$

It is evident that

$$
I(x \mid x)=H(x)
$$

The ordinary definition of entropy uses probability concepts, and thus does not pertain to individual values, but to random values, i.e., to probability distributions within a given group of values. In order to stress this difference, we will denote random values by Greek letters.
cepts. I believe that the need for attaching definite meaning to the expressions $H(x \mid y)$ and $I(x \mid y)$, in the case of individual values $x$ and $y$ that are not viewed as a result of random tests with a definite law of distribution, was realized long ago by many who dealt with information theory.
As far as I know, the first paper published on the idea of revising information theory so as to satisfy the above conditions was the article by Solomonov [1]. I came to similar conclusions, before becoming aware of Solomonov's work, in 1963-1964, and published my first article on the subject [2] in early 1965. A young Swedish mathematician, Martin-Löf, who worked in Moscow during 1964-1965, began developing this concept. His lectures [3] which he gave in Erlangen in 1966 represent a better introduction to the subject of my paper.

The meaning of the new definition is very simple. Entropy $H(x \mid y)$ is the minimal length of the recorded sequence of zeros and ones of a "program" $P$ that permits construction of the value of $x$, the value of $y$ being known,

$$
\begin{equation*}
H(x \mid y)=\min _{A(P, v)-x} l(P) \tag{2}
\end{equation*}
$$

This concept is supported by the general theory of "computable" (partially recursive) functions, i.e., by the theory of algorithms in general. We will return again to the interpretation of the notation $A(P, y)=x$.
$H(x)=\min _{P \rightarrow x}$ length $(P)$
$P_{1}=$ print
("aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa ") ;
$\mathrm{P}_{1} \rightarrow$
aaaaaaaadaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

$$
\text { length }\left(P_{2}\right)=32
$$

$P_{2}=$ for (int $\left.i=0 ; i<90 ; i++\right) p r i n t(" a ") ;$ $\mathrm{P}_{2} \rightarrow$
 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

An analogous situation exists in the principles of information theory. Essentially, it is applicable to large quantities of information, when the initial information (contained in the method on which the theory is based) is infinitesimal. Our basic formula (1) implies a "universal programming method" $A$, which exists because there are programming methods $A$ possessing the quality

$$
H_{A}(x) \leq H_{A^{\prime}}(x)+C_{A^{\prime}}
$$

They allow the programming of anything with a program length that exceeds the length of any other programming method by not greater than a constant and is dependent only on this second programming method and not on values of $x$

## Example (Mandelbrot):

- simple program
- fascinating complexity


| 0 | $\square$ | $x$ |
| :--- | :--- | :--- |




