


Computability

Paolo Baldan

University of Padua
Master's Degree in Computer Science


Gzip ...

- Year 2150. Professor Mat, a mathematician, is having a hard time in keeping track of the phone numbers of all its friends ...
- New inhabited planets are being discovered every second day, and phone numbers are becoming longer and longer ...
- How can they be stored efficiently?


Gzip ...

- Professor Hal, a computer scientist, suggests:
  "*In the phonebook, rather than the phone number itself, you might store a program that generates the number!*"
- Es.: Instead of

```
01234567890123456789012345678901234567890123456789
```

  write

```
for i=0 to 39 do print (i mod 10)
```


Gzip ...

- Is it always convenient?
- No! There are numbers n such that, for all program P generating n

$$size(n) \leq size(P)$$

$\Rightarrow$ random numbers


Gzip ...

- Mat observes "*There are infinitely many random numbers!*"
- (Why?)


Gzip ...

- Mat says: "*Hal, you could help me anyway by writing a program establishing whether a number is random or not?*"
- Hal answers "*No!*"
- But he is not unkind ...


Gzip ...

... the program does not exist!!!


Exercise

- Prove that
  - There are infinitely many random numbers
  - There is no program able to determine whether a number is random or not


We can't compute everything!

- There are **problems** which are **not solvable** by a computer ...
- These are not weird problems …
  - Halting problem
  - Program correctness
  - .....


Aim of the course

- Power and limitations of computers
- Question:
  "Which problems can we solve by a computer / by an effective procedure?"
- Intrinsic theoretical limits (independent from the specific model of computation)


Specific questions

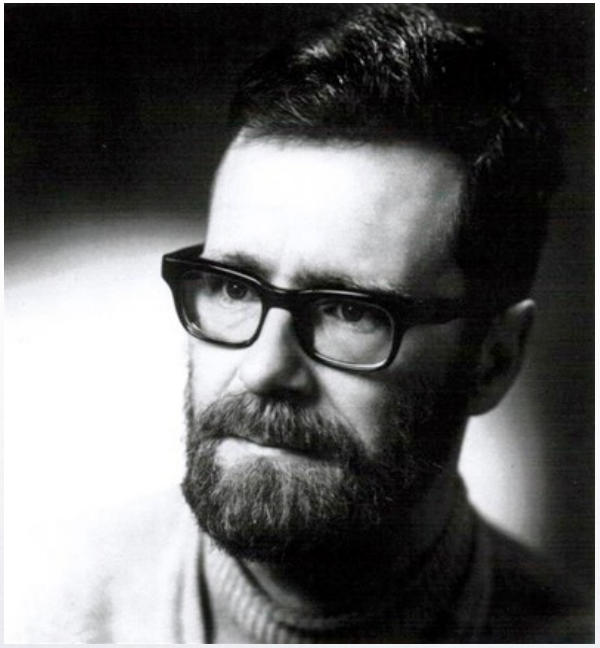
- What is an effective procedure?
- What does it means that a problem is solved by an effective procedure?
- Characterise the problems that can and those that cannot be solved
- Relating unsolvable problem (degree of unsolvability)


What about resources?

- Here we classify solvable/unsolvable problems without limitations on the use of resources (memory and time)
- Complexity theory
  - Consider resources
  - Classifies solvable problems in an hierarchy according to their "difficulty"


A brief history ...

- When did computer science start dealing with computability?
- Before its birth!
- Modern computer science started by discovering its own intrinsic limits, from an epic fail ...



What is computer science?

"Computer science is no more about computers than astronomy is about telescopes."

unsourced: Edgser Wjbe Dijkstra
[Rotterdam 1930 - Nuenen 2002]

Turing Award 1972, not an easy guy ...
the quote could well be from him

"A Case against the GO TO Statement"
letter to Communications of ACM 3, 1968

http://www.cs.utexas.edu/users/EWD/


What is computer science?

"Computer science is no more about computers than astronomy is about telescopes, biology is about microscopes, or chemistry is about beakers and test tubes. Science is not about tools. It is about how we use them, and what we find out when we do."

M.R. Fellows & I. Parberry, "SIGACT Trying to Get Children Excited About CS", Computing Research News 5(1), 1993


What is computer science?

"Computer science is the study of algorithms, including

their formal and mathematical properties
their hardware realizations
their linguistic realizations
their application"

N.E. Gibbs & A.B. Tucker, "A model curriculum for a liberal arts degree in CS", Communications of ACM 29(3), 1986 [citato da M.B. Schneider& J.L. Gersting, An invitation to Computer Science 2nd edition, 1998]


What is computer science?

- The ability of building and using tools, according to some (codified) procedure, is a distinctive feature of human beings
- Homo habilis or homus informaticus?

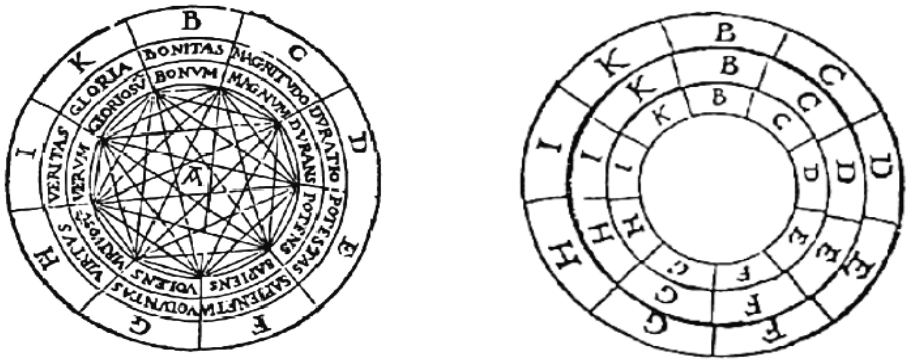

A story: Learning by mistakes

- Logics as the study of reasoning mechanisms (ability of deriving consequences from a set of premises).
- Reasoning schemes independent from the "meaning" of the single components of the sentences
  - Aristotelian syllogism: Every man is mortal, Socrates is a man thus …
- idea of a general combinatoric procedure to find all truths
- Tight link with the history of computer science

Lullus

- Raimundus Lullus (Palma de Mallorca 1232 - 1315)
  - Professor in Paris and Montpellier; Franciscan friar after a crisis of faith.
  - On *Ars Magna* (1305) he proposes a mechanical tool (Lullian wheel, designed in1275) for combining concepts and notions
    - Concepts, entities, questions, virtues, vices -> letters B-K
    - Concentric wheels to combine them
    - Once the combination is obtained, it is possible to reflect on the meaning
  - Method to refute the theses of Jews and Muslims, and convert them

Tavola 1 - Il modello delle rotule lulliane e la tavola delle dignità



Leibniz's Dream

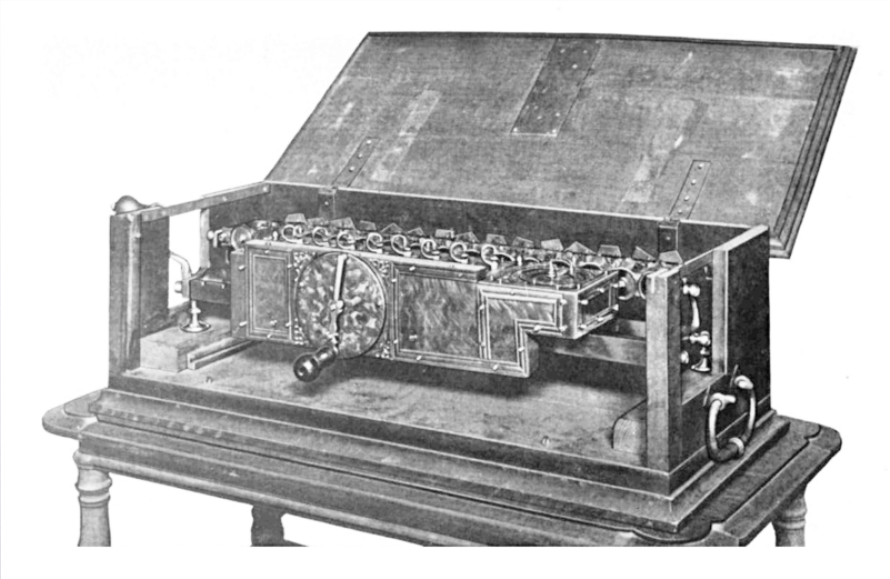
- Gottfried Wilhelm Leibniz (Lipsia 1646 - Hannover 1716)
  - "devising a language capable of perfectly representing the relations between our thoughts"
  - "philosophical" language for easing learning and development of knowledge
    - Caracteristica Universalis: universal language to express every notion and concept
      - System of symbols and basic notions (universal encyclopedia)
      - Ideal grammar for combining them (simplified Latin)
    - Calculus ratiocinator: reasoning through formal manipulation of symbols
      - ★ from reasoning about God to mathematics


Calculemus!

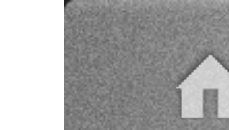
- "When controversies arise between philosophers, no discussion will be needed in the same way as accountants do not discuss. In fact, it will be sufficient to take pen and paper and say "Let's calculate!"
- Not only an abstract vision
  - Decompose the concept "man" as animal and rational, and represent the two components as prime number. E.g., assign animal to number 2 and rational to number 3. The concept of man will be expressed as 2x3 namely 6.
  - A proposition is true if, expressing the subject-predicate relationship (S / P) as a fraction, [...] the number of the subject is exactly divisible by the number of the predicate.
  - E.g., the proposition "all men are animals" reduces to the fraction 6/2 resulting in an integer (3). The proposition is therefore true.

From theory to practice

- Not only an abstract vision ("theoria cum praxis")
  - First calculating machine [the Staffelwalze, 1674] to compute the four arithmetic operations [while the Pascaline had just two], where product and division are reduced to addition and subtraction.



Maybe after the *Speeding Clock* of 1623, by Wilhelm Schickard (Herrenberg 1592 - Tubinga 1635)




Boole and his algebra

- George Boole (Lincoln 1815 - Ballintemple 1864)
  - With Leibniz, reasoning rules start to be encoded in some symbolic formalism
  - With Boole, logics is interpreted as an algebra
    - In the statements "Every plant is a living being" and "Every man is mortal" plants, living being, human, mortal are seen as classes
    - Boolean algebra provides the laws for these classes
  - For instance …
    - x = animals that are sheeps, y = white entities, x*y = white sheeps !!

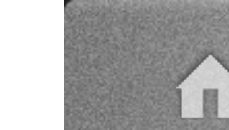

Boole and his algebra

- Laws about classes, in particular (as in Leibniz)
  - x * x = x
- Algebra of logic = ordinary algebra restricted to 0, 1 (interpreted as the empty and universal class, respectively)
- Interpretation for + and -
  - x + y = entities that are in class x or in y [same for x - y]
- With simple algebraic manipulations …
  - x * x = x ---> x - x * x = 0 ---> x * (1 – x) = 0

...“principle of non-contradiction” from Aristotle's Metaphysics (it is impossible that a quality belongs and does not belong to the same entity).

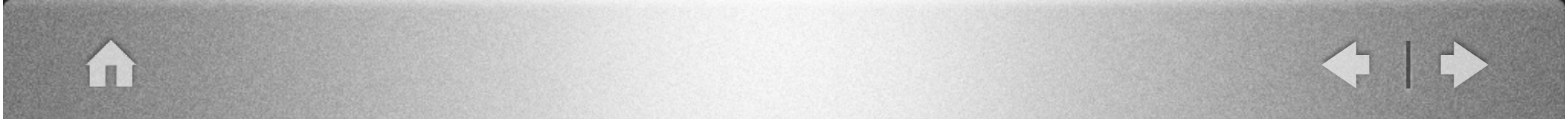
detour

- Charles Babbage (Londra 1791 - Marylebone 1871)
  - We will not discuss of Babbage (neither of Aiken and its Harvard Mark I-IV)
  - Difference Engine (n.II: project 1849; costructione 1991) is a *special purpose* machine for computing polynomials based on the finite difference method [from f(1) derive f(1.1) etc.], since multiplication was not allowed ...
  - Analytical Engine (from 1837 onward) is a *general purpose* machine, programmable (punched cards), with memory and arithmetic unit (*mill*)
    - Never realised, essentially forgotten until 1930s, it left us the name of a language (ADA, from Ada King, Countess of Lovelace) and good science fiction …

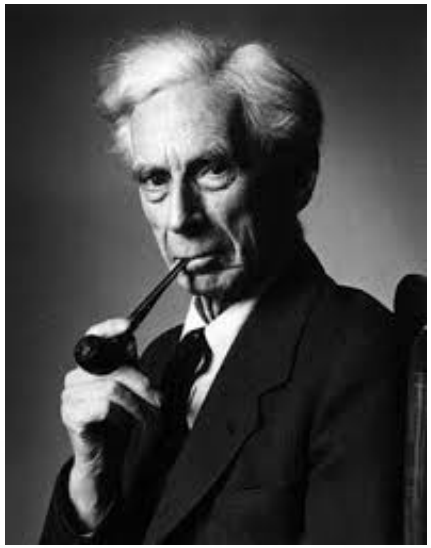



Frege

- Gottlob Frege (Wismar 1848 - Bad Kleinen 1925)
  - Boole's logic represented a branch of mathematics that included logical reasoning ... circularity !!
  - Frege placed logic as the foundation of all mathematics
    - Ideography (*Begriffsschrift*, 1879: formal calculus of symbols, 100p): artificial formal language with syntactic and manipulation rules (predicate logic)
      - variables & quantification
        - all horses are mammals: $\forall x\ horse(x) \Rightarrow mammal(x)$
        - some horses are black: $\exists x.\ horse(x) \wedge black(x)$
  - Letter from Russel (1902): interesting, but... inconsistent! [$\{ x \mid x \notin x \}$]



Russel's paradox



- Define

$$R = \{x \mid x \notin x\}$$

- Problem: $R \in R$?
  - YES, $R \in R$
    hence *R* does satisfy the defining property $R \notin R$
  - NO, $R \notin R$
    hence *R does not* satisfy the defining property $R \in R$

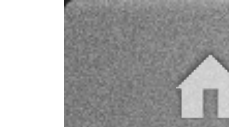

In this course we won't use slides

Hilbert

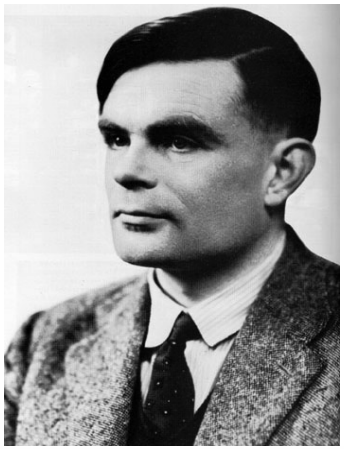
- David Hilbert (Wehlau 1862 - Gottinga 1943)
  - Formal rephrasing of Leibniz's dream, without metaphysical ambitions
    - Math (starting from geometry: *Grundlagen der Geometrie*, 1899) reduced to a formal system (axioms + rules)
    - Consistency (as a foundation for existence, opposed to constructivism) to be proved with finitistic tools
  - Entscheidungsproblem (EP, "decision problem"), expressible as
    - "given a complete system [for first order logic], give a decision algorithm [that determines whether a formula is provable]"


Godel breaks the dream!

- Kurt Gödel (Brno 1906 - Princeton1978)
  - Terrible blow for Hilbert's logicistic program
  - Incompleteness theorems for arithmetic (1931)
    - First: in every axiomatizable and consistent theory T of elementary arithmetic there are sentences F for which one cannot prove neither "F" nor "not F" (intuitively, neither the falsity nor the truth of F can be proved)
    - Second: Under the same hypotheses, in T one cannot prove the consistency of T itself.




Turing continues …



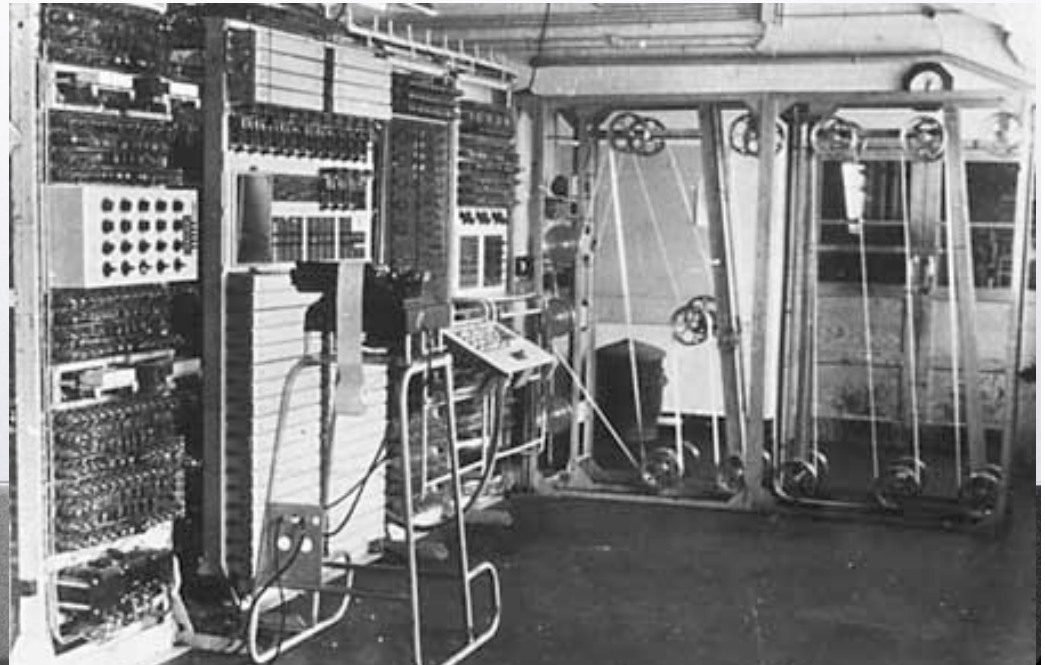
- Alan Turing (London 1912 - Wilmslow 1954)
  - Turing machine (MdT)
    - Machine that reads / writes symbols on a tape guided by a "program": starting from input data it produces an output
  - Formalization of the notion of computing procedure
    - Algorithm: very ancient concept...
      - Euclid (Greece, 300-400 BC): Algorithm for GCD
      - Al-Chwarizmi (Persia, 800 BC): Algorithms for operations in decimal notation

Turing (cont.)

- TM
  - Solid notion of computable function
    - TM computes everything that is computable (Church-Turing thesis)
  - But it can't computer everything
    - Halting problem: Given a program P and an input x, does the execution of P on x terminate?
  - (Hilbert) deductions as computable functions -> negative answer to EP
- Existence of a universal TM [*general purpose machine*]
  - accepts as input data and the description of a TM [program], expressed in the same language, and executes the program on the data
  - Univ(x,y) executes the program x on the datum y

Turing (cont.)

- He worked in 1943 in Bletchey Park at the Colossus (special purpose computer for deciphering Nazi codes), understanding the potential of electronics
- Contributes to the design of the first programmable computer
  - Never realised since beyond the technological limits (6k memory!!!)
  - Unknown for the need to keep military secret (the existence of Colossus revealed in the 70s)



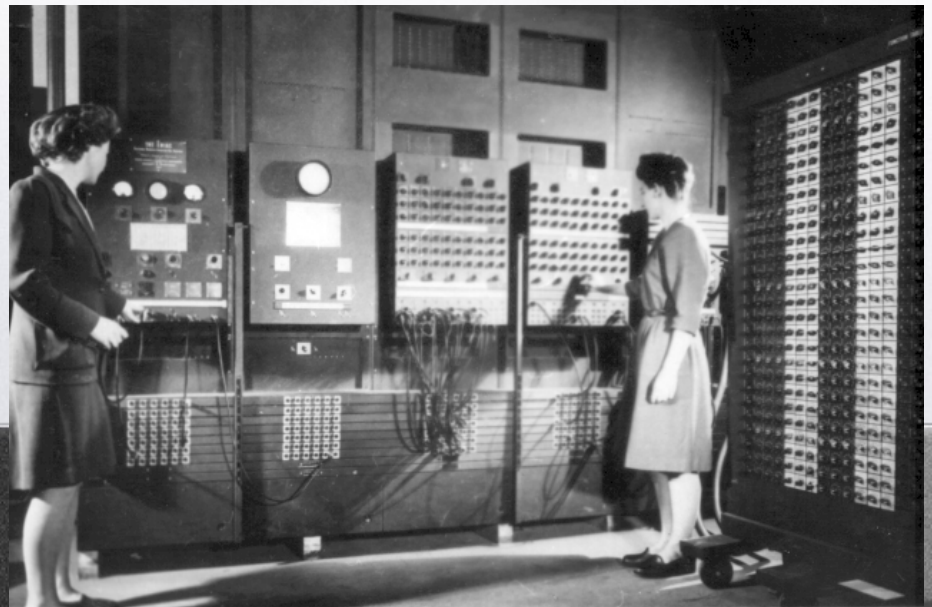
Colossus X

Modern computer

- John Von (János) Neumann (Budapest 1903 - Washington 1957)
  - The idea of Universal TM (program and data in memory) leads to the modern programmable digital computer
  - EDVAC (Electronic Discrete Variable Automatic Computer) Report of 1945 remembered as the origin of the computer
  - [Turing was quite ahead and we should also mention Konrad Zuse (Berlino 1922 - Hünfield 1992), with his Z3 ...]

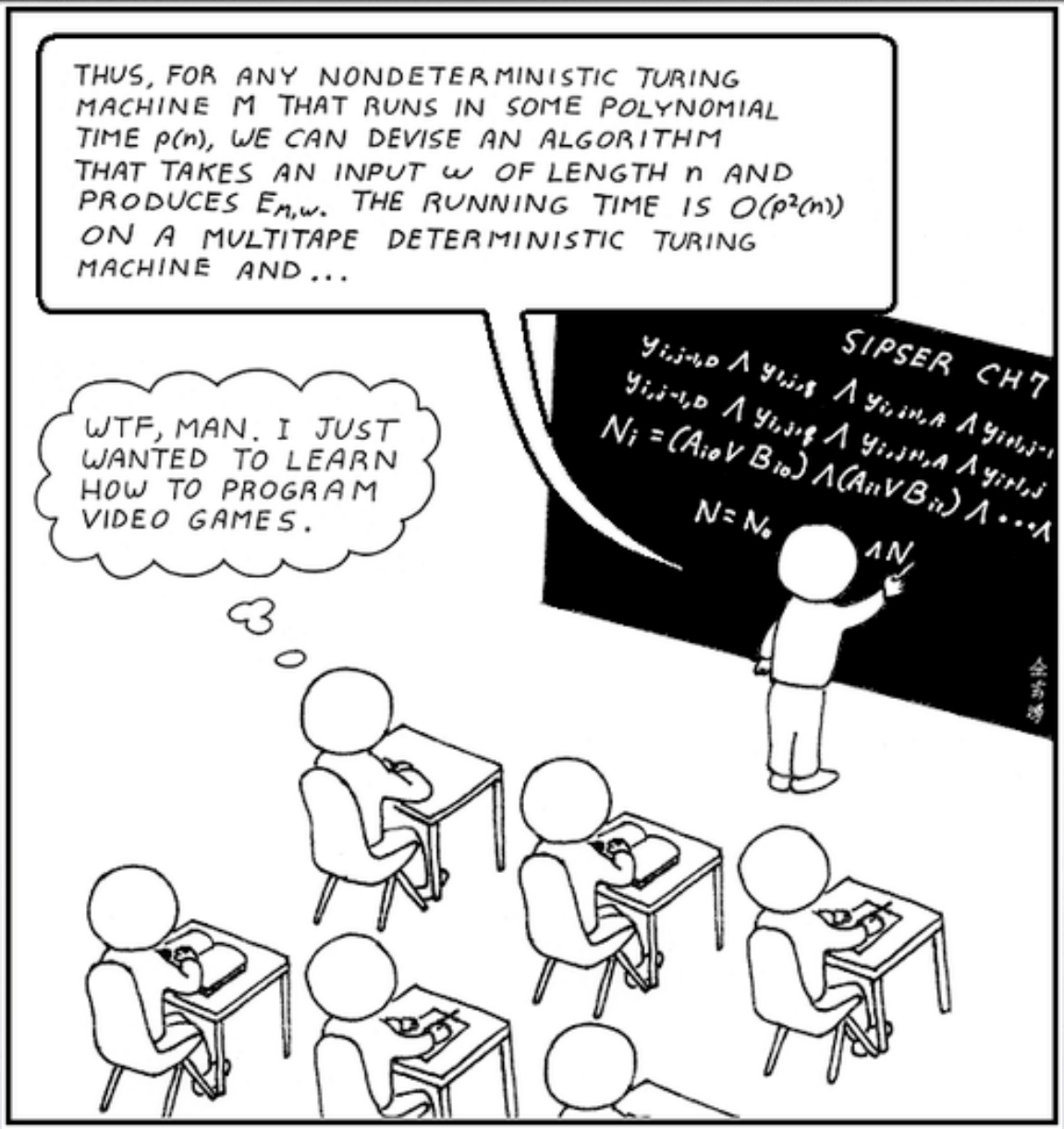
Modern computer

- 1946: ENIAC (Electronic Numerical Integrator And AND A Computer), designed by John Presper Eckert and John Mauchly
- 1949: EDVAC
- 1951: UNIVAC I (UNIVersal Automatic Computer I) is the first commercial computer (business and management) in the USA




Message

- Computability theory is
  - at the convergence of a fascinating intellectual adventure
  - of interest to various disciplines
  - determines the birth of modern computer science


THUS, FOR ANY NONDETERMINISTIC TURING MACHINE M THAT RUNS IN SOME POLYNOMIAL TIME p(n), WE CAN DEVISE AN ALGORITHM THAT TAKES AN INPUT w OF LENGTH n AND PRODUCES $E_{M,w}$. THE RUNNING TIME IS $O(p^2(n))$ ON A MULTITAPE DETERMINISTIC TURING MACHINE AND...
WTF, MAN. I JUST WANTED TO LEARN HOW TO PROGRAM VIDEO GAMES.
SIPSER CH7
$N = N_0 \wedge N$


Info on the course

- Schedule
  Lun, Mar (8:30-10:15), first semester
- Book: Nigel Cutland "Computability"
  Cambridge University Press
- Web Page:
  http://www.math.unipd.it/~baldan/Computability
  + Moodle
  https://stem.elearning.unipd.it/course/view.php?id=6539


Info on the course

- Office hours for students:
  Just fix an appointment
- Tutoring:
  Dr. Giacomo Stevanato
- Exam
  Written test (Exercises)
  + "optional" oral discussion