Aalto University
School of Science

CS-C2160 Theory of Computation

Appetizer: Computational Problems, Models of Computation

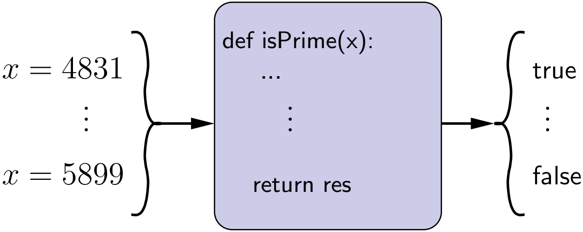
Pekka Orponen
Aalto University
Department of Computer Science

Spring 2021

Computational Problems

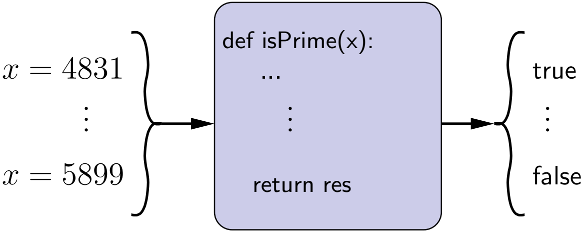
Computational Problems

Can one make a program that detects whether a given number x is a prime number? (Very large primes are important in cryptography.)



Computational Problems

Can one make a program that detects whether a given number x is a prime number? (Very large primes are important in cryptography.)



Answer: Yes, a very inefficient way is to just go through all the pairs of integers in $\{2,...,x-1\}$ and check that their product does not equal x.

Computational Problems

Can one make a program that tells whether a multivariate polynomial equation system has a *real-valued* solution?

$$\text{eqns=}\ \begin{array}{r} 3x^2y^4+1<0 \\ y>0 \end{array}$$

$$\vdots$$

$$\text{eqns=}\ \begin{array}{r} x^2+y^2-1<0 \\ -4xy-4x+y-1>0 \\ x^3+2x^2+3y^2-5<0 \end{array}$$

$\longrightarrow$

```
def solve(eqns):
    ...
      ⋮

    return res
```

$\longrightarrow$

false

$\vdots$

true $(x=-0.5, y=0)$

Computational Problems

Can one make a program that tells whether a multivariate polynomial equation system has a *real-valued* solution?

$$\text{eqns}= \begin{array}{r} 3x^2y^4+1<0 \\ y>0 \end{array}$$

$$\vdots$$

$$\text{eqns}= \begin{array}{r} x^2+y^2-1<0 \\ -4xy-4x+y-1>0 \\ x^3+2x^2+3y^2-5<0 \end{array}$$

```
def solve(eqns):
    ...
      ⋮

    return res
```

false

$\vdots$

true $(x=-0.5, y=0)$

Answer: Yes, but this is not easy, see e.g. this report.

Computational Problems

Can one make a program that tells whether a multivariate polynomial has *integer-valued* roots?

$$p = 3x^2y^4 + 1$$

$$\vdots$$

$$p = x^3 + y^3 + z^3 - 29$$

$$p = x^3 + y^3 + z^3 - 33$$

```
def hasIntRoots(p):
    ...
       ⋮

    return res
```

false

$\vdots$

true $(x = 3, y = 1, z = 1)$

?

Computational Problems

Can one make a program that tells whether a multivariate polynomial has *integer-valued* roots?

$$\left.\begin{array}{r} p = 3x^2y^4 + 1 \\ \vdots \\ p = x^3 + y^3 + z^3 - 29 \\ p = x^3 + y^3 + z^3 - 33 \end{array}\right\} \longrightarrow$$

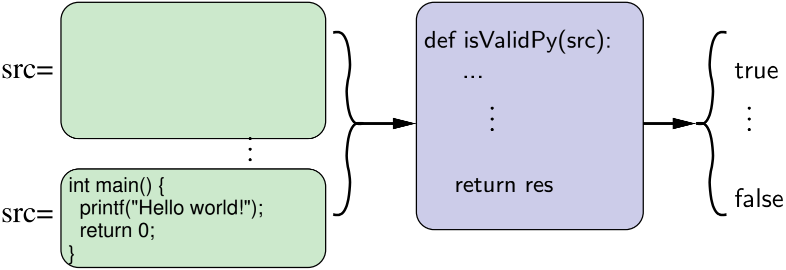
```
def hasIntRoots(p):
    ...
        ⋮

   return res
```

$$\longrightarrow \left\{\begin{array}{l} \text{false} \\ \vdots \\ \text{true } (x = 3, y = 1, z = 1) \\ \text{?} \end{array}\right.$$

Answer: No, this is called Hilbert's tenth problem and it cannot be solved by a computer.

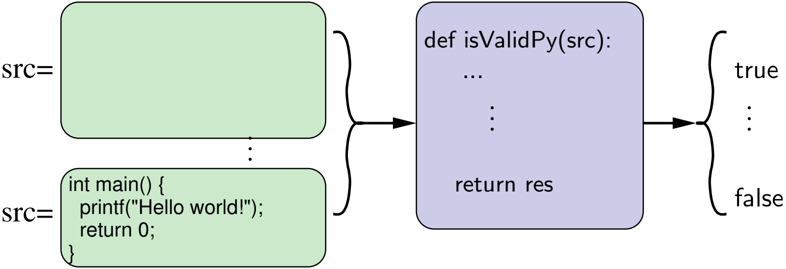
Computational Problems

Can one make a program that tells if a text file is a valid Python program?



Computational Problems

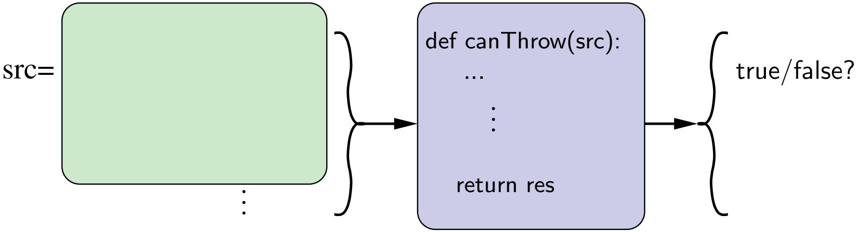
Can one make a program that tells if a text file is a valid Python program?



Answer: Yes, the Python interpreter/compiler does this as the first step.

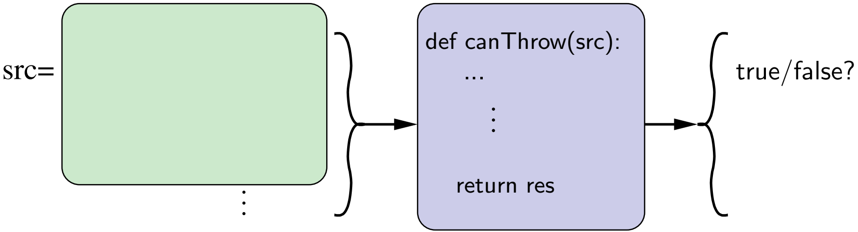
Computational Problems

Can one make a program that tells if there exists an input that causes a given Python program to throw an exception, e.g. `ZeroDivisionError`? (Such a program would be a very convenient "perfect compiler", able to detect all possibilities for run-time errors in advance.)



Computational Problems

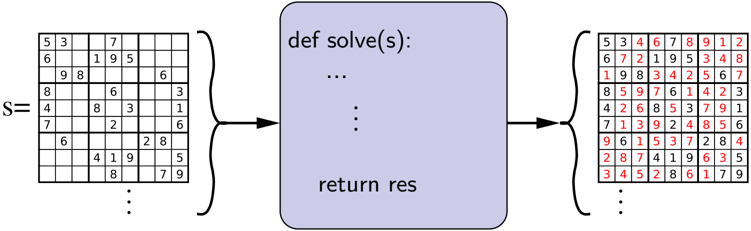
Can one make a program that tells if there exists an input that causes a given Python program to throw an exception, e.g. `ZeroDivisionError`? (Such a program would be a very convenient "perfect compiler", able to detect all possibilities for run-time errors in advance.)



Answer: Assuming that the source Python program can access unlimited memory resources, this is not possible.

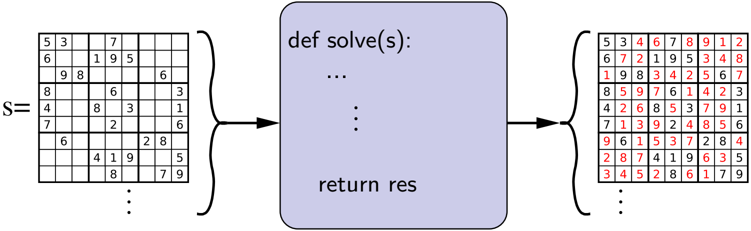
Computational Problems

Can one make a program that solves sudokus?



Computational Problems

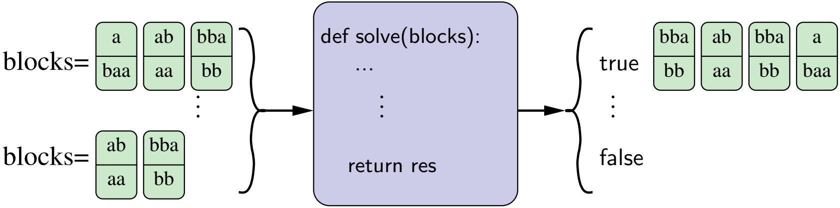
Can one make a program that solves sudokus?



Answer: Yes, an inefficient way is to just enumerate through all the solution candidates.

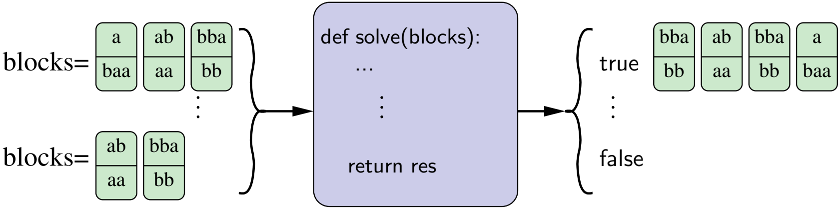
Computational Problems

Can one make a program that decides whether blocks from a given set (multiple copies are allowed) can be organised so that the top and bottom row have the same string?



Computational Problems

Can one make a program that decides whether blocks from a given set (multiple copies are allowed) can be organised so that the top and bottom row have the same string?

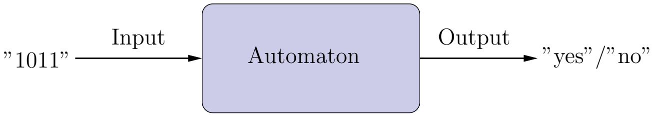


Answer: No, this is called Post's Correspondence Problem and it cannot be solved by a computer.

Models of Computation

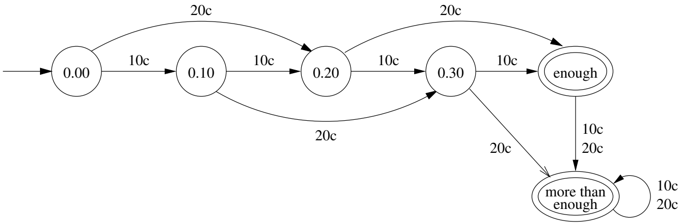
Problem: To answer these kinds of questions, we need a model of a computer/computer program.
Question: Mathematical model of a computer/computer program?
This course:

- Different classes of automata that process input.
- The inputs "accepted" by an automaton form its language.
- Also: grammars (duals of automata) generating the same languages.



E.g. the language of a primality testing automaton would be $\{2, 3, 5, 7, 11, 13, 17, 23, \ldots\}$

Model I: Finite state automata



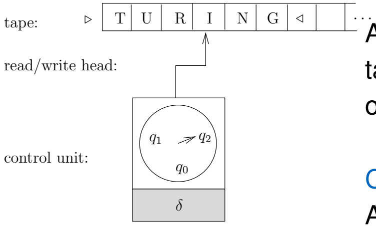
- Finite amount of memory
- Can only read input, one step at time

Application areas of variants:

- Communication protocols
- Simple embedded controllers
- Lexers in compilers (e.g. recognising keywords etc. when compiling Java to bytecode)
- ...

Model II: Turing machines

Turing machines (Alan Turing 1935–36)

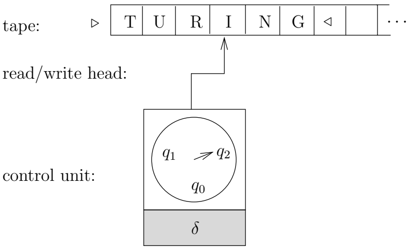


A finite state automaton with an unbounded tape that it can read, write, and move left/right one step at time.

Church-Turing thesis:

Any mechanically solvable problem can be solved with a Turing machine.

Model II: Turing machines



A Turing machine is a 7-tuple

$$M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}}),$$

where:

- Q is a finite set of *states*;
- Σ is the *input alphabet*;
- $\Gamma \supseteq \Sigma$ is the *tape alphabet* (s.t. $\triangleright, \triangleleft \notin \Gamma$
- $\delta : (Q - \{q_{\text{acc}}, q_{\text{rej}}\}) \times (\Gamma \cup \{\triangleright, \triangleleft\}) \to Q \times (\Gamma \cup \{\triangleright, \triangleleft\}) \times \{L, R\}$ is the *transition function*;
- $q_0 \in Q$ is the *initial state*;
- $q_{\text{acc}} \in Q$ is the *accepting state*; and
- $q_{\text{rej}} \in Q$ is the *rejecting state*.

FAQ: Why do we need all these symbols and formal definitions?

Answers:

- To precisely communicate complex constructions (concepts, problems, algorithms, etc) to other people.
- To make solid, mathematical arguments about properties of constructions.
  - In the general case, this problem cannot always be solved because ...
  - This problem is computationally difficult because ...
  - My algorithm outputs "yes" if and only if the input ...

Some interesting courses to continue after this course

- CS-E3190 Principles of Algorithmic Techniques
- CS-E4530 Computational Complexity Theory
- CS-E4320 Cryptography and Data Security
- Many other CS courses