

CS 361: Theory of Computation

Lecture 1: Introduction & Logistics

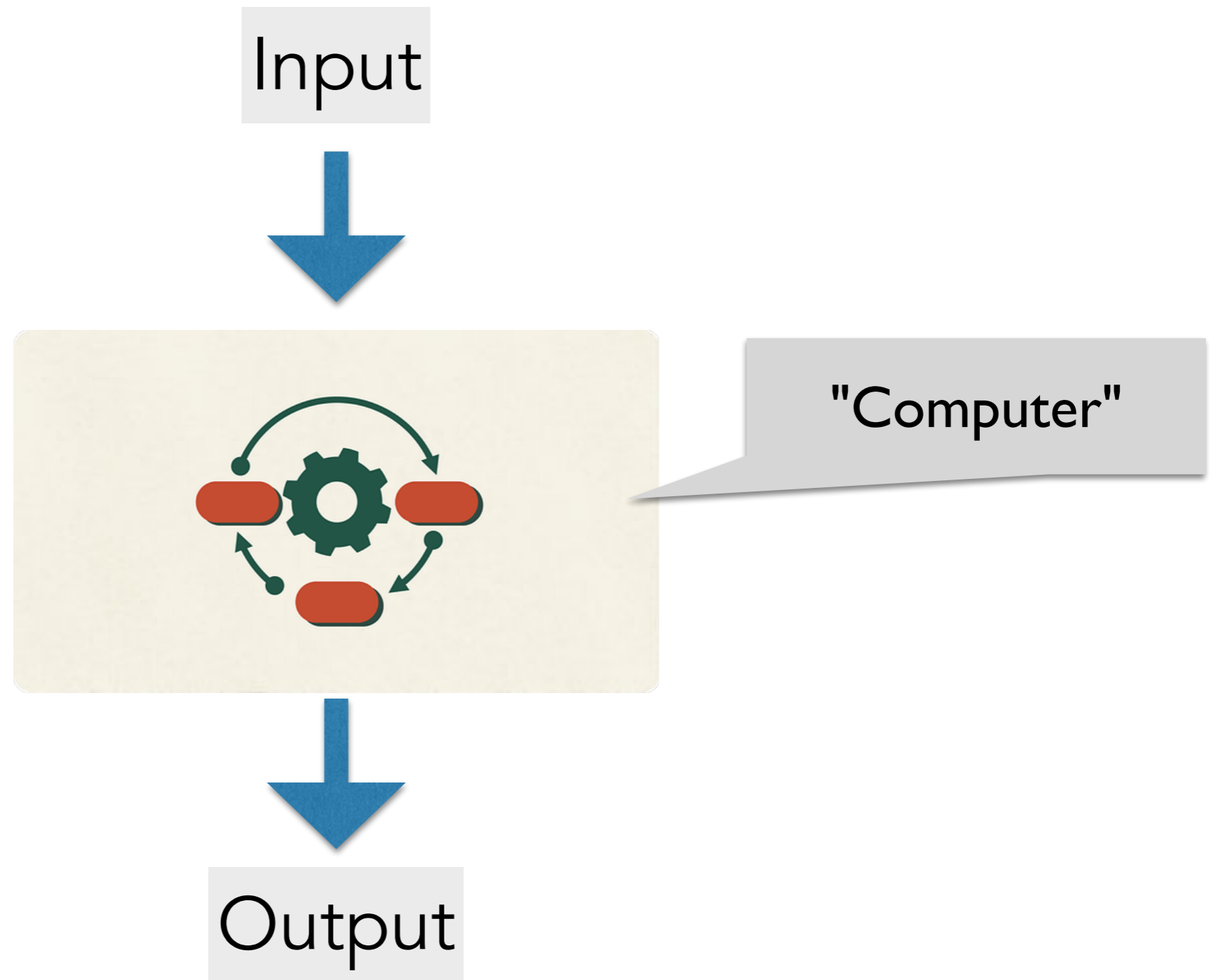
Shikha Singh

Introductions

What is Theory of Computation?

What is Computation?

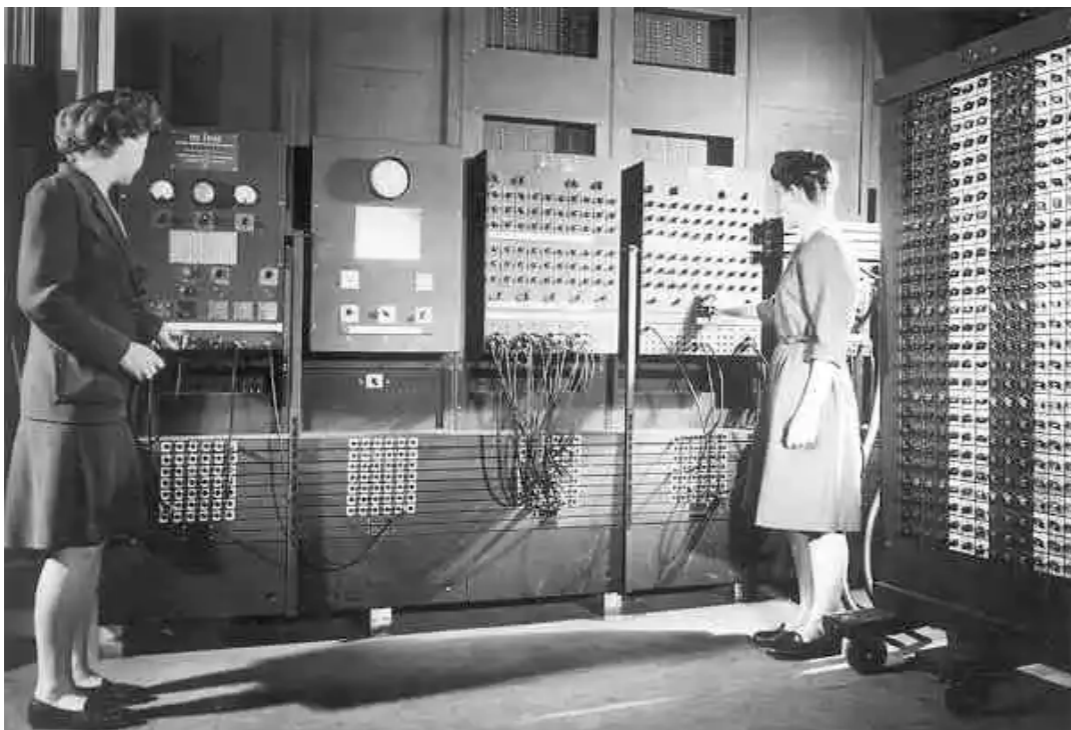
What is Computation



Computers Now



Computers: Early 20th Century



Algorithms are Ancient

- Algorithms have been around for thousands of years
- Grade-school multiplication algorithm was invented by Babylonians
- Euclid's GCD algorithm (~300 BC)

$$\begin{array}{r} \\ \\ x \\ \hline \\ \\ \\ \hline \\ \hline \end{array}$$

```
1: procedure GCD(a, b)
2:   while a ≠ b do
3:     if a > b then
4:       a ← a − b
5:     else
6:       b ← b − a
7:     end if
8:   end while
9:   return a
10: end procedure
```


How Do We Define an Algorithm?

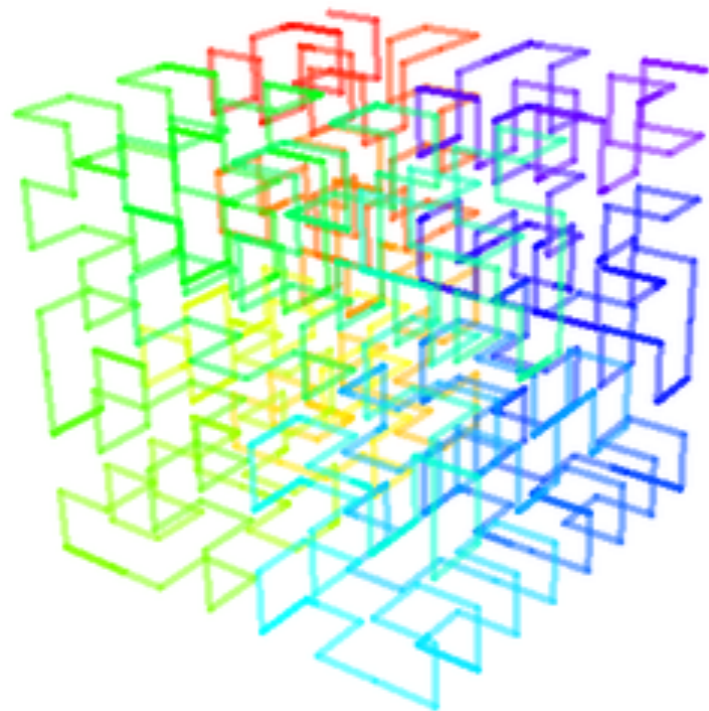
- What constitutes an algorithm? How do we define it?
 - Intuitively, step by step process
 - That eventually terminates and produces the desired output
- To design algorithms, this intuitive understanding was sufficient
- Components of an algorithm:
 - **Specification:** What is the task the algorithm performs
 - **Implementation:** How is the task accomplished
 - **Analysis:** Is it correct? Is it efficient?
- **Question.** Can all problems be solved by some algorithm?

Theory of Computation

- Need a formal model of what it means to solve a problem
- Theory of Computation:
 - Building a mathematical model for computation
 - Using the model to understand the power and limits of computation
 - Gain insights that inform applications

Where it Started: Hilbert's Challenges

- **[1900-1930]** David Hilbert identifies several mathematical problems as the challenges for the coming century
- Two of these problems concerned Computer Science



1862 - 1943

Hilbert's 10th Problem

- Hilbert's 10th problem [1900]:
 - Given a multivariate polynomial with integer coefficients, is there a **process that determines in a finite number of operations** whether the equation has an integral solution

$$3x^2 - 2xy - y^2z - 7 = 0$$

$$x = 1, y = 2, z = -2$$

Integer solution

$$x^2 + y^2 + 1 = 0$$

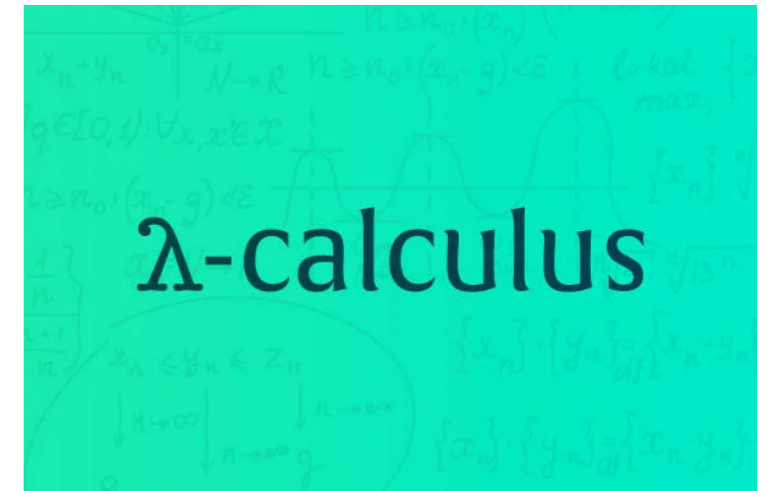
No solution

Hilbert's Entscheidungsproblem

- Hilbert believed the answer was yes but many attempts failed
- To show it was not solvable, more formalization was needed of what it means to use a "finite procedure" to solve a problem
- **Hilbert's Entscheidungsproblem** (Decision problem) [1928]:
 - **Is there a finite procedure** that determines whether a given mathematical statement is true or false?
- Hilbert again believed the answer was yes:
 - There was no such thing as an unsolvable problem

Attempts to Define Computation

- **[1930s: Post, Gödel, Church]** attempt to solve Hilbert's Entscheidungsproblem
- Post machine, lambda calculus, Gödel machine



Emil Post



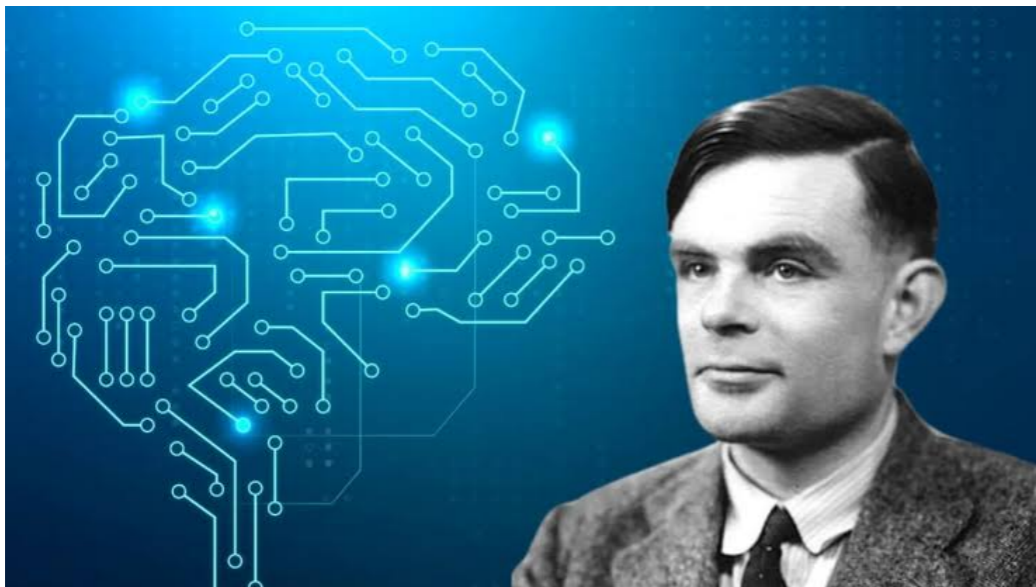
Kurt Gödel



Alonzo Church

Birth of Computer Science

- **[1936]** As a graduate student Alan Turing (at age 24) devised what is now called the Turing machine and used it to devise an uncomputable problem
- Church and Turing:
 - λ -computable \equiv Turing computable



230 A. M. TURING [Nov. 12,

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO
THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

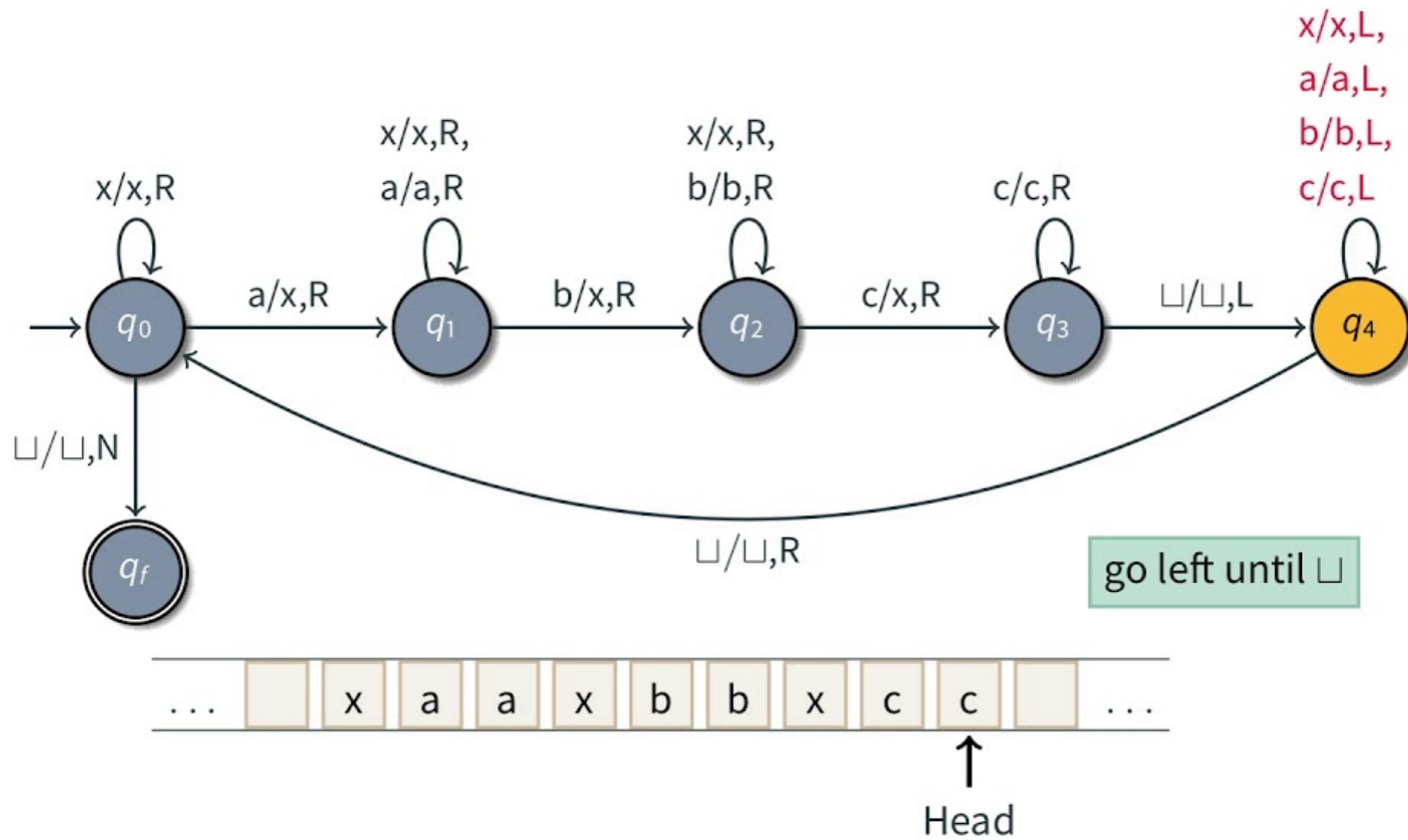
[Received 28 May, 1936.—Read 12 November, 1936.]

The “computable” numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable *numbers*, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbersome technique. I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers. According to my definition, a number is computable if its decimal can be written down by a machine.

In §§ 9, 10 I give some arguments with the intention of showing that the computable numbers include all numbers which could naturally be regarded as computable. In particular, I show that certain large classes of numbers are computable. They include, for instance, the real parts of all algebraic numbers, the real parts of the zeros of the Bessel functions, the numbers π , e , etc. The computable numbers do not, however, include all definable numbers, and an example is given of a definable number which is not computable.

Although the class of computable numbers is so great, and in many ways similar to the class of real numbers, it is nevertheless enumerable. In § 8 I examine certain arguments which would seem to prove the contrary. By the correct application of one of these arguments, conclusions are reached which are superficially similar to those of Gödel†. These results

† Gödel, “Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I”, *Monatshefte Math. Phys.*, 38 (1931), 173–198.

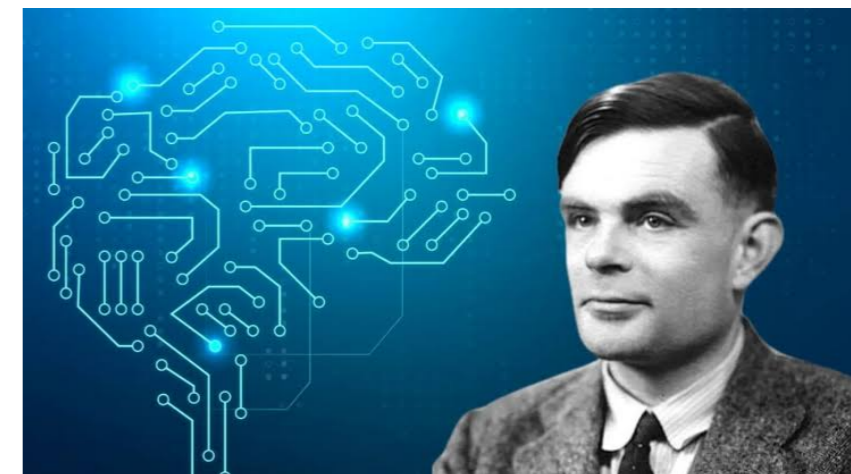
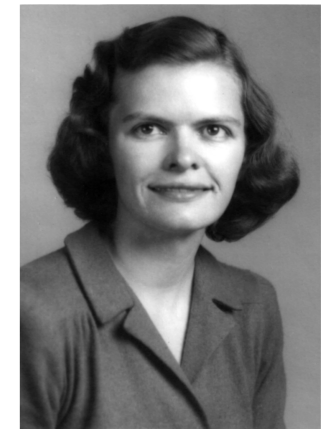
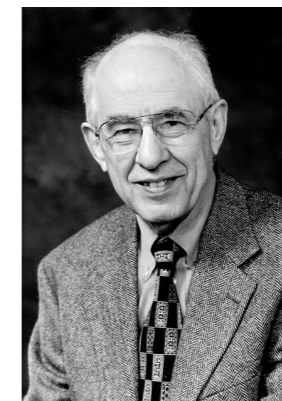
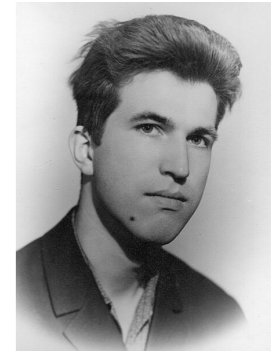


Church and Turing Thesis

- Turing machines predates modern computer as we know it, yet there is no existing physical model that cannot be modeled by it
- **Church-Turing Thesis:**
 - Intuitive notion of "computable" is captured by functions computer by a Turing machine
 - **[Physical CT Thesis]** Any computational problem that can be solved by any physical process, can be solved by a Turing machine

Hilbert's Challenges: Conclusion

- Hilbert's 10th problem [1900]:
 - Given a multivariate polynomial with integer coefficients, is there a **process that determines in a finite number of operations** whether the equation is solvable
 - **No:** Martin Davis, Yuri Matiyasevich, Hilary Putnam and Julia Robinson [1970]
- Hilbert's Entscheidungsproblem (Decision problem) [1928]:
 - **Is there a finite procedure** that determines whether a given mathematical statement is true or false?
 - **No:** Alan Turing [1936]



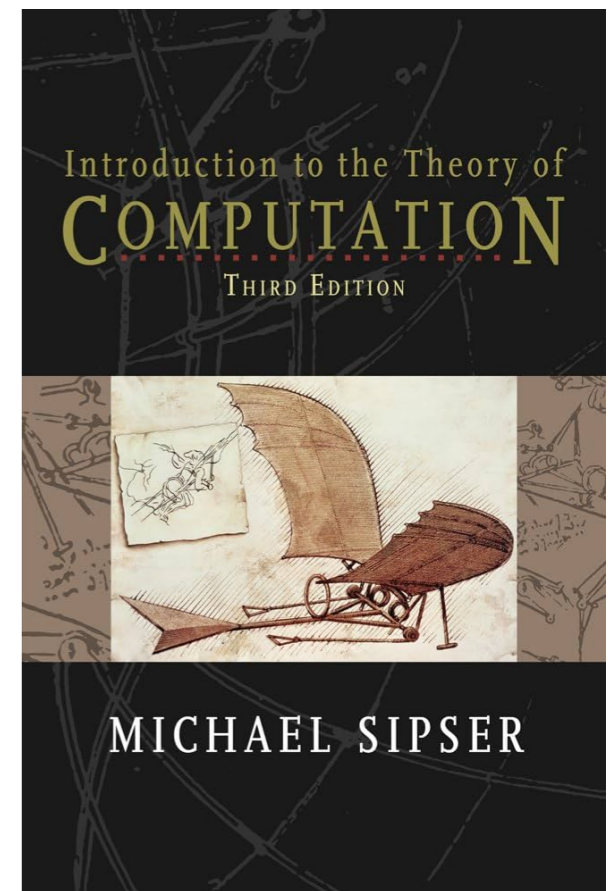
Computability and Complexity

- **Computability** of a problem:
 - Can a problem be solved by a given computational model
 - Start with restricted models: automaton
 - Build up to Turing machines (modeling modern computers)
- **Complexity** of a problem:
 - Is there an efficient algorithm to solve it?
 - Efficiency: time and space complexity
 - Practice with reductions
 - Study the hierarchy of these classes

Course Logistics

Textbooks

- Primary: Introduction to Theory of Computation (3rd ed) by Sipser
 - Will follow it pretty closely
 - Reserved at Schow if you need it
- Supplemental readings:
 - Introduction to Theoretical Computer Science by Boaz Barak
 - Online: <https://introtcs.org/public/index.html>



Course Webpage

- Link: <https://williams-cs.github.io/cs361-f24/index.html>
- Lecture materials, readings and assignments will be posted here
- Will occasionally use GLOW for internal documents

CSCI 361 - Fall 2024

Theory of Computation

[Home](#) | [Lectures](#) | [Assignments](#) | [Resources](#) | [CS@Williams](#)

Home

Instructor:	Shikha Singh
Email:	ss32@williams.edu
GLOW page:	CSCI 361 GLOW
Office Hours:	Check the calendar below.
Lectures:	TR 8:30 am - 9:45 am (01) and TR 9:55 am - 11:10 am (02).
Classroom	Wachenheim 116
Textbook	Introduction to the Theory of Computation by Michael Sipser (3rd ed)

Course Description

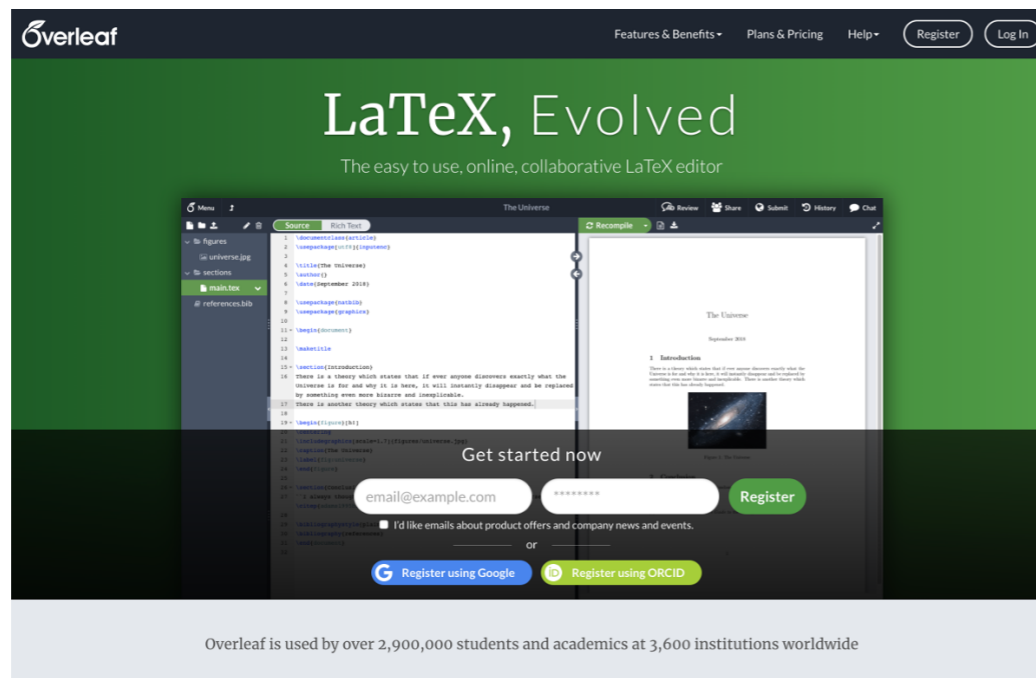
This course introduces a formal framework for investigating both the computability and complexity of problems. We study several models of computation including finite automata, regular languages, context-free languages, and Turing machines. These models provide a mathematical basis for the study of computability theory. The class also explores important topics in complexity theory: hardness of problems and reductions and characterizations of time and space complexity classes.

Syllabus and Grade Breakdown

- Posted on course webpage
 - <https://williams-cs.github.io/cs361-f24/handouts/syllabus.pdf>
- Grading breakdown:
 - Assignments (30 %)
 - Attendance, Readings & Class Participation (10 %)
 - Survey paper and presentation (10 %)
 - Midterm Exam (25 %)
 - Final Exam (25 %)

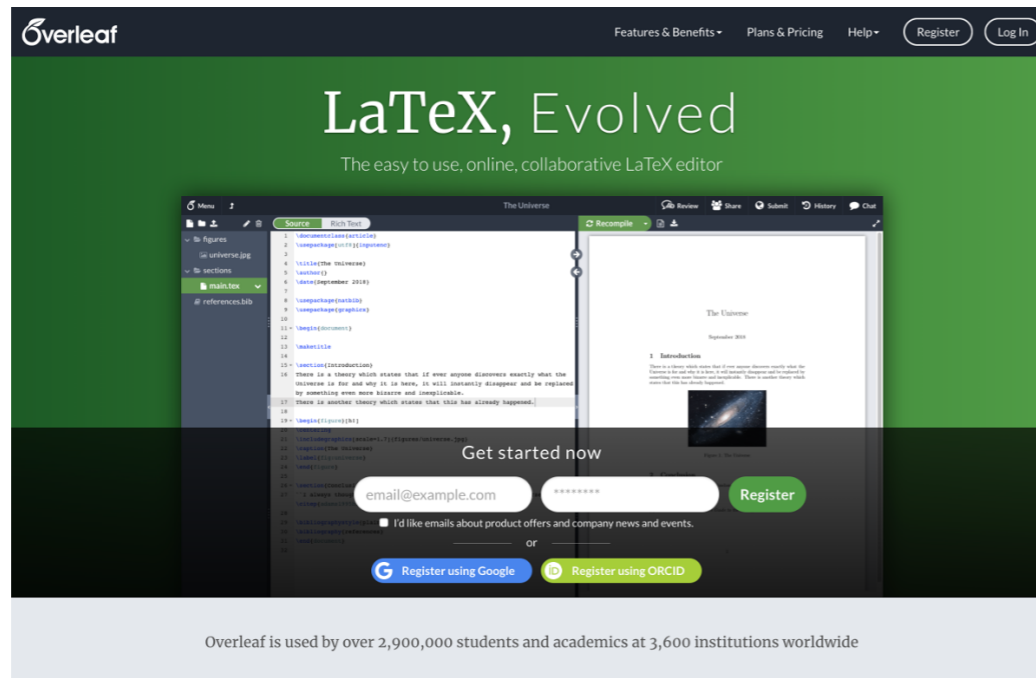
Problem Sets

- Problem sets for practicing concepts from class
- Must be typeset in LaTeX (using provided template in Overleaf)
- Anonymized grading: no name/ID on HWs
- Submit via Gradescope (Course ID: **844447**)
- Assignments will typically be released on Thursdays and due on Wed



Assignment 1

- First assignment will be released early next week and due Sept 17 (*Tues*, instead of *Wed*) because I am traveling Wed Sept 18-20
- Typically assignments will be due Wed



Attendance, Readings & Class Participation

- Early morning class!
- Incentive to attend and come prepared
 - **Reading HW:** brief, pencil and paper question based on reading
 - Hand in at the beginning of class
 - Count as attendance (required)
 - Only graded on completeness
- Everyone can miss two-sessions at no penalty
- Otherwise, if you need to miss, reach out ahead of time

Grab next lectures reading assignment on the way out!



About Class Participation

- I like interaction in my classes!
- Most lectures will include in-class problem solving
 - Think of them as mini labs
- This is a small classroom
 - Unusual in CS but great for in-class activities
- This can be a great learning experience for you if you help build a good community in class
 - Be a good teammate, come prepared and help each other!

Bottom line. *Help create a vibrant, positive, and inclusive classroom environment!*

Survey on Advanced Topic

- Many fun advanced topics you can explore at the end
- Chance to choose one you like with a partner
 - Learn more about it
 - Present to your classmates in class
 - Submit a brief report
- Will provide options of topics and associated readings
- Think of it as a low stakes mini project:
 - Provides flexibility for creativity and exploration
 - Focus is on learning rather than building something

Honor Code

- Read: academic honesty section of the syllabus
- Gist:
 - Collaboration is encouraged and you can discuss high-level ideas, clarifications, examples to understand the question, etc
 - Should not discuss low-level details
 - Not allowed to search the internet/ChatGPT with question specific prompts
 - At best, these take away valuable learning opportunities
 - At worst, they are confusing and damaging to your learning
- You must arrive at on your own and understand the work you submit

Bottom line. *Any work that is not your own is a violation of the Honor Code.*

Course Support

- Instructor Office Hours:
 - Mon, Tues and Wed: 2.30 - 4 pm
- Two TAs: Leah Williams and Nathaniel Tunggal
 - TBD: will be posted on the course webpage soon

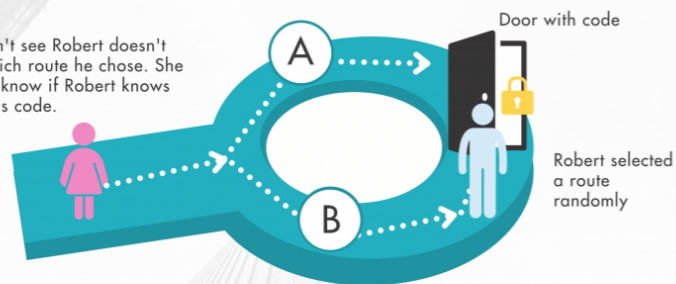


Course Outline

- Week 1: Background, Sets and Languages
- Week 2-3: Finite Automaton and Regular Languages
- Week 4: Non-regularity and context-free grammars
- Week 5-7: Turing machines and computability
- Week 8-10: Time and Space Complexity, Reductions
- Week 11-12: Advanced topics, student presentations

Zero-knowledge proof

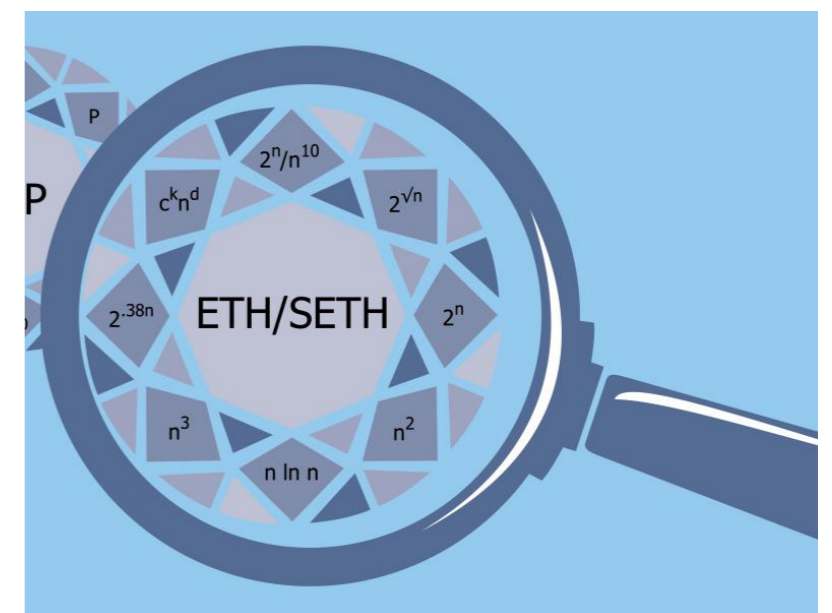
• Mary can't see Robert doesn't know which route he chose. She wants to know if Robert knows the door's code.



• Mary randomly tells Robert a route back. If Robert returns by the route Mary said it would prove that Robert probably knows the code.

• The higher the number of attempts, the less likely it is that Bob will be able to guess the path Mary will choose and the more likely he is to actually know the code.

MANGROVIA
SOLUTIONS



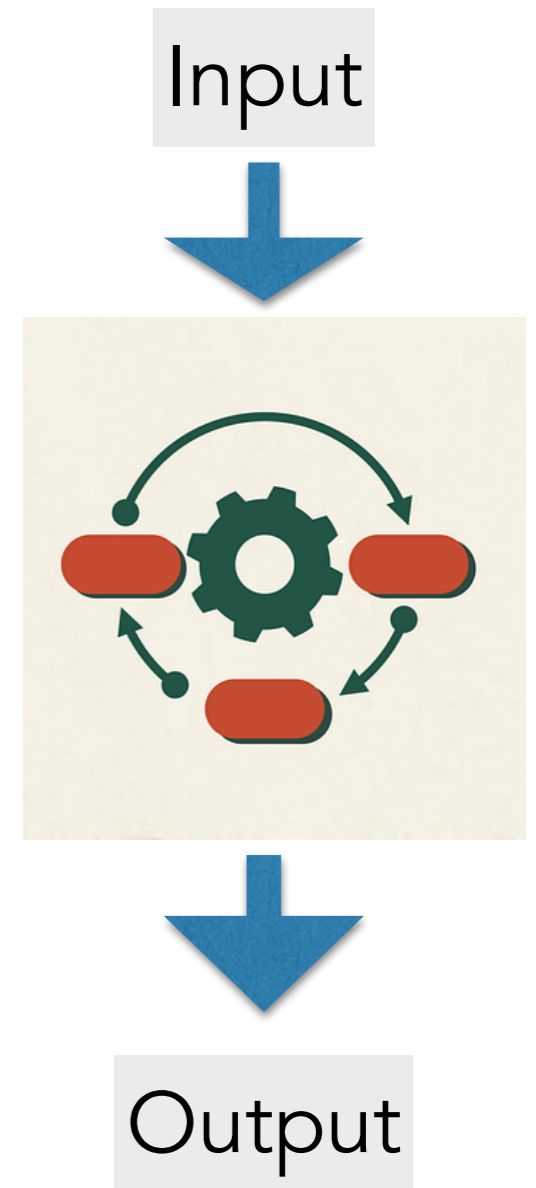
Is this Stuff Useful?

- Typical computer scientist attitude: urgency to "build"
- CSCI 361 is not about building or coding, but....
 - Concepts have stood the test of time and led to many insights
 - Old paradigm: Good theory informs good practice
- Also, concepts in this course have proved particularly applicable
 - **Automaton & RegEx** → Scanners, circuit design, cellular automaton
 - **Context-free grammars** → Building parsers for compilers
 - **Computability and halting program** → Program verification
 - **Formal systems and logic** → Foundation of AI and Databases
 - **Complexity Theory** → Cryptography and Security

Data Representation

Representing Data

- Mathematically modeling input/output?
- Input/output can be any object:
 - Images, text, electrical signals, social network, etc
- What is the typical approach in CS?
 - "Encode" this data into text/strings
 - Specifically binary strings



Encodings

- Not specific to CS languages:
 - Spoken languages encode objects through words to represent them
- Does the choice of alphabet matter?
- **Alphabet** Σ = a non-empty and finite set made up of symbols
- **String** s : a finite (possibly empty) sequence of symbols from Σ
 - $s = a_1a_2\cdots a_n$ where each $a_i \in \Sigma$
- Binary strings with $\Sigma = \{0,1\}$
 - ϵ (empty string)
 - 01, 000, 1110000...111

A B C D E
F G H I K
L M N O
P Q R S T
V X Y Z

अ आ इ ई उ ऊ
ऋ ॠ लृ लृ
ए ऐ ओ औ
क ख ग घ ङ
च छ ज झ ञ
ट ठ ड ढ ण
त थ द ध न
प फ ब भ म
य र ल व
श ष स ह

Strings: Definitions

- **Length** of a string s :

$$|s| = \text{the number of symbols in } s$$

- Σ^* = set of all finite-length sequences over Σ

- Example:

- $\{0,1\}^* = \{\epsilon, 0, 1, 00, 01, 10, 11, 000, \dots\}$

- $\{a\}^* = \{\epsilon, a, aa, aaa, \dots\}$

- **Note:** Σ^* is an infinite set, but each string in it has a finite length

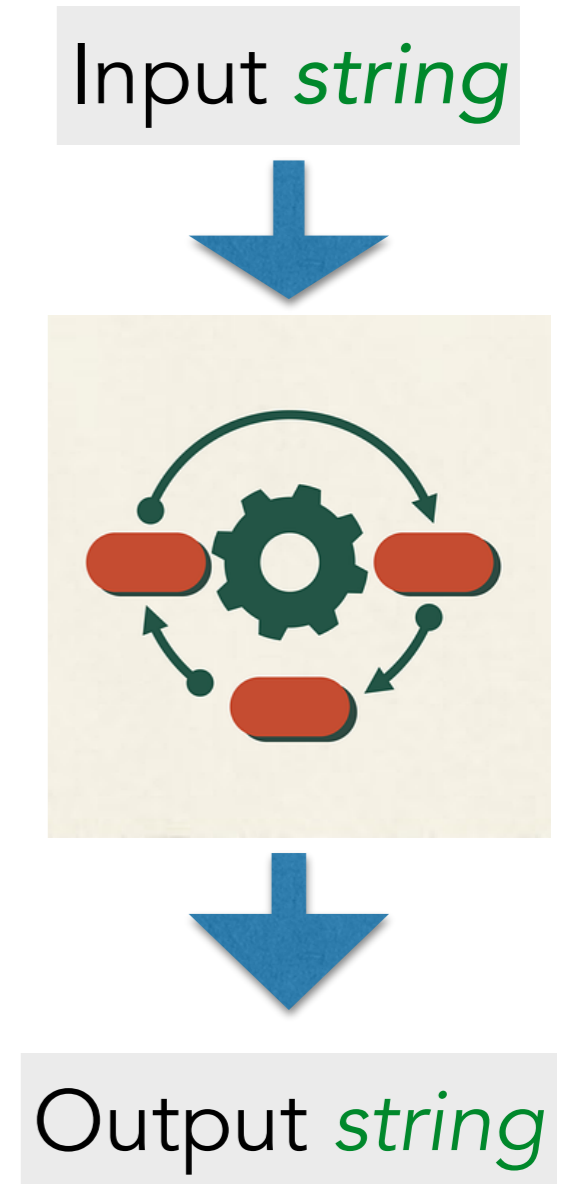
Encoding: Definition

- Given a set A of objects, an **encoding** is an injective (one-to-one) function that maps A to Σ^*
 - No two objects have the same encoding
- Restricting to binary alphabet:
 - Can encode an alphabet with $|\Sigma| = k$ in binary using $\lceil \log_2 k \rceil$ bits
 - This extra factor is constant wrt size of input
- **Question.** Can we encode everything?
 - Encodability = Countability (will come back to this)
- How do we encode **uncountable** sets (e.g. \mathbb{R})?
 - Approximation (with some precision)

Takeaway: In theory of computation, all input/output data is a string

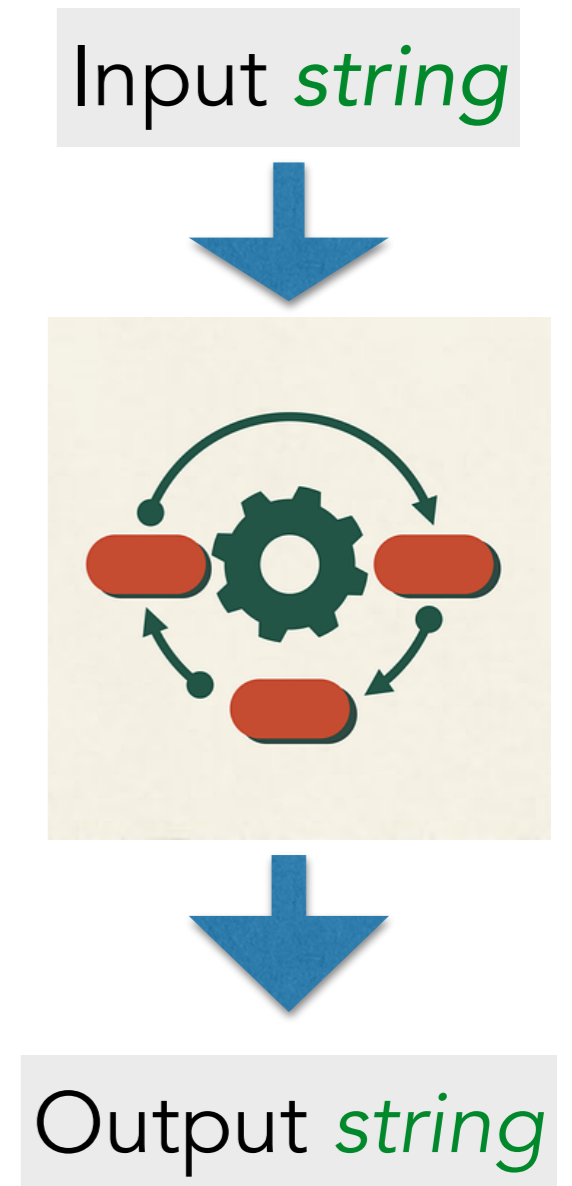
Back to Computation

- Input and output are strings over an alphabet
 - Input can be any finite length string
 - Output is a finite length string
- Now we need to define computation
 - For every input, there is an output
- What mathematical object captures this?
 - A function f from $\Sigma^* \rightarrow \Sigma^*$
- **Question.** Is computation just a function?
 - We need to know **how** to transform the input to the output



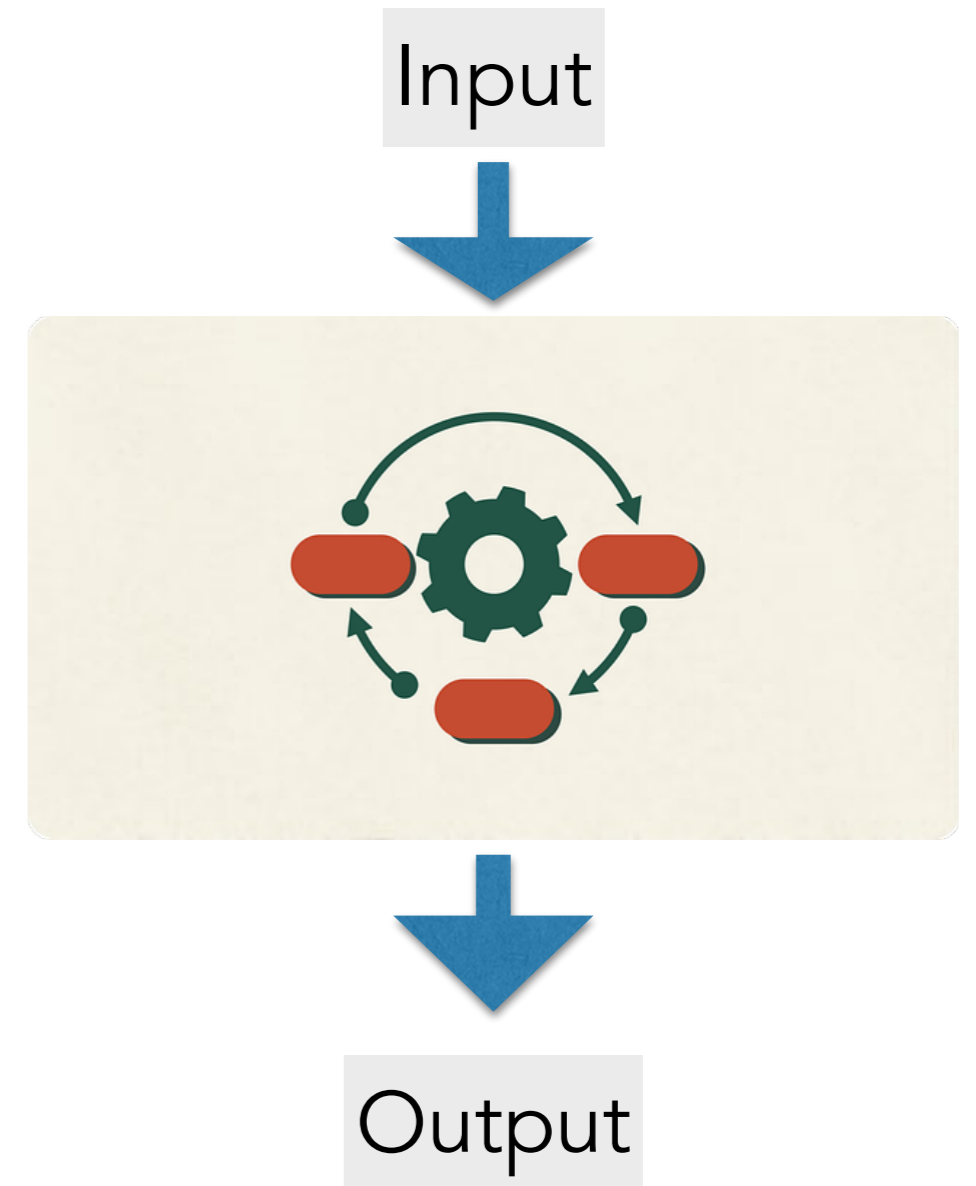
Function Problem

- Specification of a computational problem
- Function problem:
 - A function of the form $f : \Sigma^* \rightarrow \Sigma^*$
 - Specifies input, output pairs
- A computer/algorithm **solves** function problem f if its input/output behavior matches f
- Examples:
 - Reverse function
 - Sort function
 - isPrime



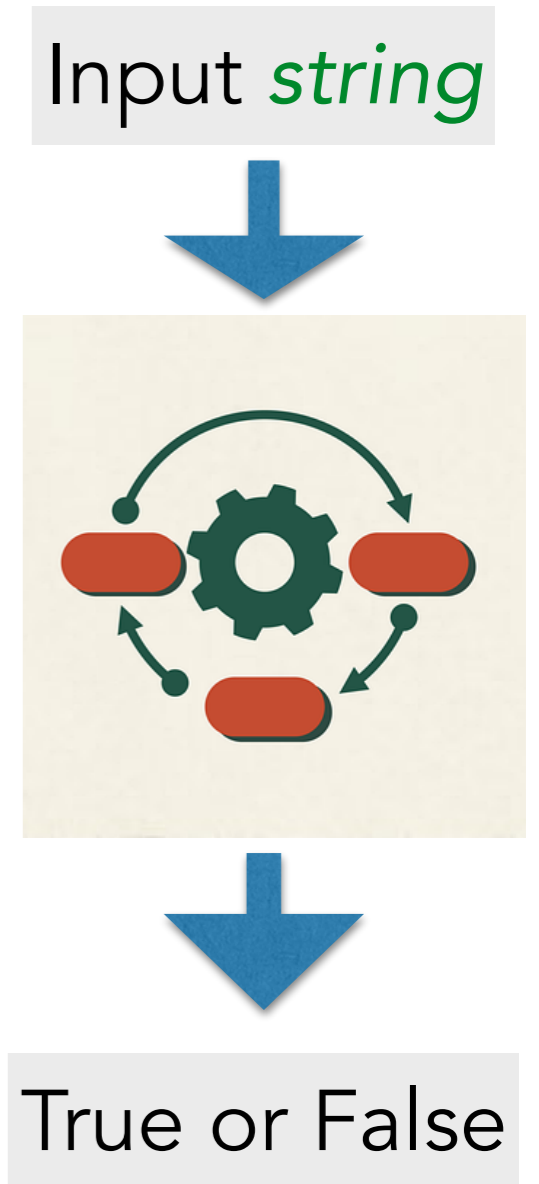
Takeaways: Defining Computation

- **Computation:** manipulation of information/data to solve a problem
- **Computational problem:** the input/output pairs
- **Algorithm:** description of how this data is manipulated



Decision Problem

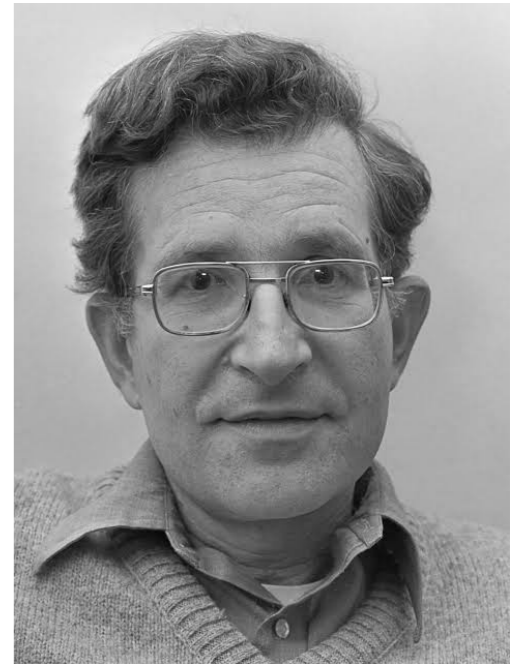
- A further convenient restriction on output:
 - Only consider decision problems
- A decision problem is a function $f: \Sigma^* \rightarrow \{0, 1\}$
- Examples:
 - Given a graph, is there a clique of size k ?
 - Given a number, is it prime?
- This restriction simplifies the study of computation, without losing much



Languages

- Language: any **set** L of finite-length strings over an alphabet Σ
 - That is, any set $L \subseteq \Sigma^*$
 - Intuitively, a language is set of words over an alphabet
- Examples for $\Sigma = \{0, 1\}$
 - $L = \emptyset$
 - $L = \Sigma^*$
 - $L = \{1, 01, 001, 0001, \dots, \}$
- One-to-one mapping between decision problem f and language L :
 - $f(s) = 1$ if and only if $s \in L$

Influence of Chomsky



- We will study computation through the lens of languages
- Influence of linguist Chomsky on computation
- A **grammars generates** a language (akin to speaking)
 - Any string in the language can be generated using the rules of the grammar
- A **machine recognizes** a language (akin to listening)
 - If a given input string is in a language, the machine will "accept" (output true), otherwise "reject" (output false)

