THEORY OF COMPUTATION
CS363, SJTU

Xiaofeng Gao
Dept. of Computer Science
Shanghai Jiao Tong University

Outline

- What is Theory of Computation?
- History of Computation
- Branches and Development

THEORY OF COMPUTATION

The Essential Question

- Back to 1930's, mathematical logicians first began to explore the meaning of computation, using one question——

  What are the fundamental capabilities and limitations of computers?

Definition

- In theoretical computer science, the theory of computation is the branch that deals with whether and how efficiently problems can be solved on a model of computation, using an algorithm.
- Three major branches
  - Automata Theory
  - Computability Theory
  - Computational Complexity Theory

Automata Theory

- The study of abstract mathematical machines and the computational problems that can be solved using these machine
- Automata → Greek word (Αυτόματα)
  - something is doing something by itself
- Play a role in several applied areas of CS
  - Finite automation: text processing, compilers, hardware design
  - Context-free Grammar: programming languages, artificial intelligence

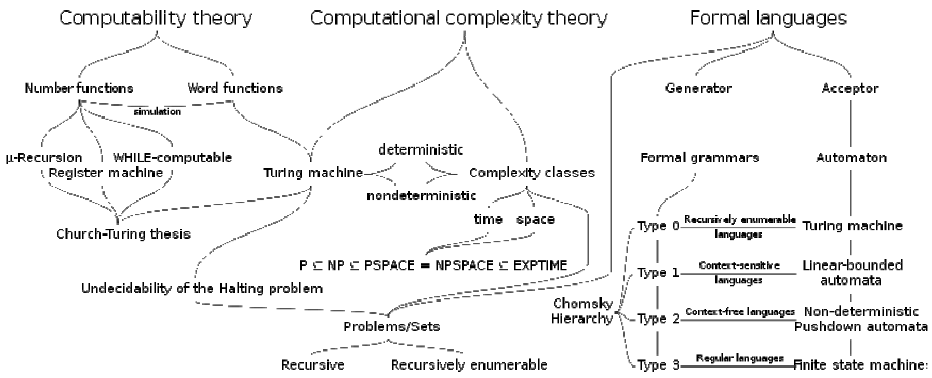
Computability Theory

- What problem is solvable on a computer?
  - Whether a mathematical statement is true/false
  - Halting Problem (easy to formulate, impossible to solve by TM)
  - Rice's Theorem
    For all non-trivial properties of partial functions, it is undecidable whether a Turing machine computes a partial function with that property.
- Closely related to recursion theory
  - Theoretical models of computers
  - Lead to the construction of actual computers

Computational Complexity Theory

- Given a problem, how much resource do we need to compute it?
  - How efficiently the problem can be solved
  - Execution time (Time Complexity)
  - Memory space (Space Complexity)
- Classify the difficulty of computer problems
  - E.g., Complexity classes P and NP
  - ***What makes some problems computationally hard and others easy?***

Relationship



HISTORY OF COMPUTATION

Gottfried Leibniz (1646-1716)

- Leibniz's Law
  - Identity of indiscernibles
  - Anticipate modern logic and analytic philosophy
  - Formal logic / Symboic logic
- Principles of Leibniz's logic
  - All our ideas are compounded from a very small number of simple ideas.
  - Complex ideas proceed from these simple ideas by a uniform and symmetrical combination.

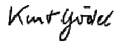
Germany

David Hilbert (1862-1943)

Germany

- Hilbert's 23 Problems
  - International Congress of Mathematicians in Paris in 1900
- 2^{nd}: Prove that the axioms of arithmetic are consistent.
  - The compatibility of arithmetical axioms
  - Consistency
  - Completeness
- Foundational Crisis of Mathematics
  - Russell's paradox

Kurt Gödel (1906-1978)



- Gödel's Complete Theorem
  - 1929
  - First Order Logic (predicate calculus)
- Gödel's Incomplete Theorem
  - 1931
  - On Formally Undecidable Propositions of "Principia Mathematica" and Related Systems
- for any computable axiomatic system that is powerful enough to describe the arithmetic of the natural numbers (Peano axioms), that:
  - If the system is consistent, it cannot be complete.
  - The consistency of the axioms cannot be proven within the system.

Alan Turing (1912 – 1954)

UK

- Foundation of Computation Theory
  - On Computable Numbers, with an Application to the Entscheidungs Problem (decision problem), 1936
- Turing Machine
  - the most powerful possible "reasonable" model of computation
  - reformulated Kurt Gödel's universal arithmetic-based formal language
- Turing Award
  - 1966
  - Association for Computing Machinery (ACM)

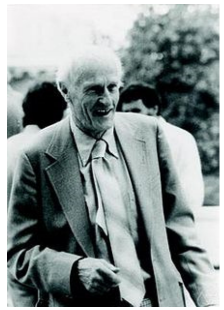
Alonzo Church (1903 – 1995)

- Lambda Calculus (λ-calculus)
  - a way to formalize mathematics through the notion of functions, in contrast to the field of set theory
- Church–Turing thesis
  - Everything algorithmically computable is computable by a Turing machine

USA

Stephen Kleene (1909 – 1994)

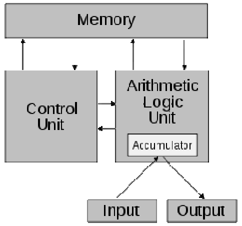
- Church's Student
- Founder of Recursion Theory
  - Kleene hierarchy
  - Kleene algebra
  - Kleene star (Kleene closure)
  - Kleene's recursion theorem
  - Kleene fixpoint theorem



John von Neumann (1903 – 1957)

- Logical Design of EDVAC
  - 1945 (101 pages)
  - First Draft of a Report on the EDVAC
- Von Neumann architecture
  - Referential model
  - processing unit
  - arithmetic logic unit
  - processor registers

Hungarian-American



Hartmanis and Stearns

- On the computational complexity of algorithms (1965)
  - Foundation of Computational Complexity
  - TIME(f(n))
  - Time Hierarchy Theorem
- Derandomization
- Hardness of approximation
- Interactive proof system

Stephen Cook (1939 -)

- University of Toronto
- The Complexity of Theorem Proving Procedures (1971)
  - Polynomial-time reduction
  - NP-completeness
  - P vs. NP problem
- Turing Award (1982)
  - Feasibly Constructive Proofs and the Propositional Calculus

USA

The Future …

- Distributed & Parallel System
- Approximation & Randomization
- Algorithmic Game Theory
- ……

THANK YOU!