Algebra powers computation

Nitin Saxena (CSE@IIT Kanpur, India)

(*Thanks to the artists for their images.)

December 2022, INAE-BARC, Mumbai

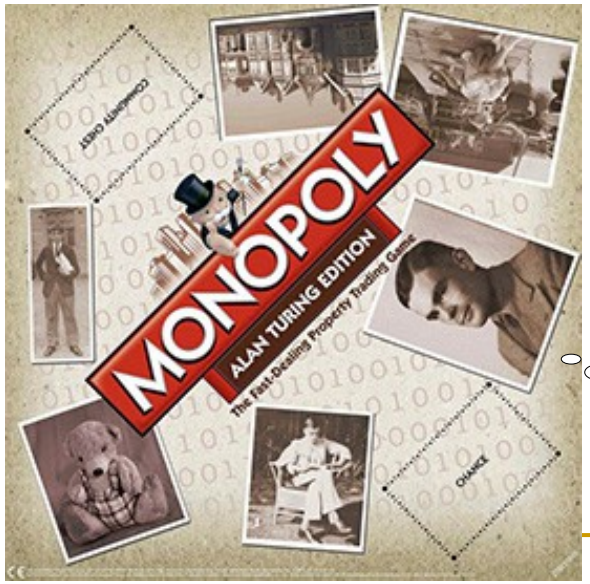
Contents

- Church & Turing
- Valiant: Algebraic circuits
- Zero or nonzero: PIT
- Soundbite

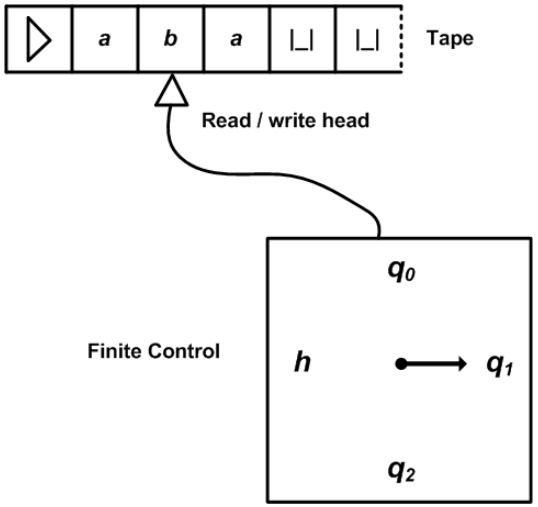
What's computing?

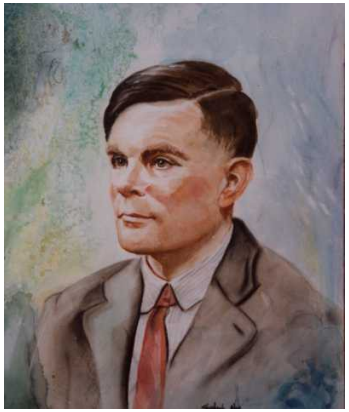
- The first response was by Alonzo Church (1935-6).
  - Using effective computability based on his λ-calculus.
- Soon, Alan Turing (1936) postulated a simple, most general, mathematical model for computing – Turing machine.

Church (1903-1995)



100th bday!
2012.





Turing (1912-1954)

Church & Turing


Hilbert (1862-1943)

- Computation is: whatever can be simulated on a Turing machine (TM).
- TM invented to resolve Hilbert (1928)'s question--

  "***design an <u>algorithm</u> to decide whether a given statement is provable from the axioms using logic".***

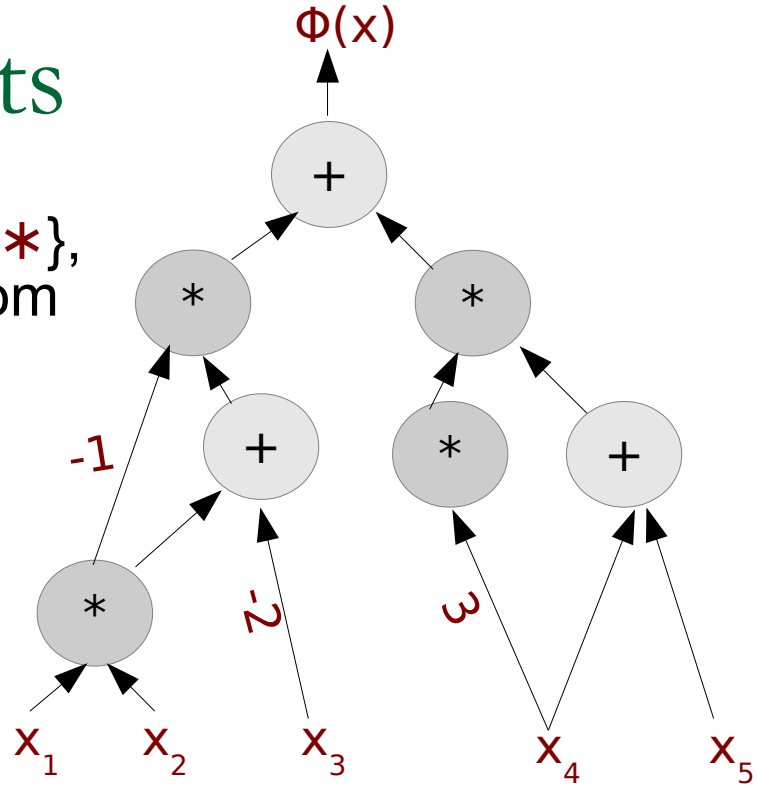
  Entscheidungsproblem
- The answer requires defining 'algorithm'.
  - hence, 'computation' requires a new mathematical framework.
- Algorithm is very much like a *program*.
  - TM is like a *real computer*-- highly iterative & trivial steps.

Contents

- Church & Turing
- Valiant: Algebraic circuits
- Zero or nonzero: PIT
- Soundbite

Valiant: Algebraic circuits

- An arithmetic circuit Φ has gates $\{+, *\}$, variables $\{x_1,....,x_n\}$ and constants from some field F.
- An arithmetic circuit is an *algebraically neat model* to capture real computation.



- Valiant (1977) formalized computation & resources using algebraic circuits.
  - Giving birth to his VP≠VNP question.
  - Or, the algebraic hardness question!

Leslie Valiant (1949-)

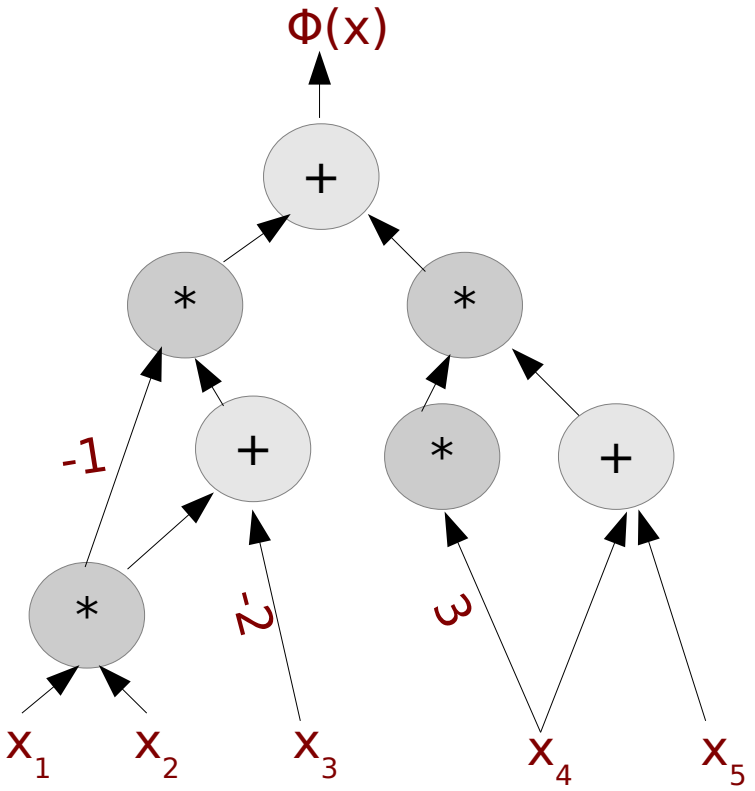
Contents

- Church & Turing
- Valiant: Algebraic circuits
- Zero or nonzero: PIT
- Soundbite

Zero or nonzero: PIT

- Question: Test whether a given circuit is *zero*.
  - Polynomial identity testing (PIT).
- OPEN Qn: Is PIT in deterministic polynomial time?
- Work in last decades show:

Meta-Theorem: A solution of identity testing would answer the hardness question.



Contents

- Church & Turing
- Valiant: Algebraic circuits
- Zero or nonzero: PIT
- Soundbite

Works-- PIT inspired

- Blackbox algorithms for various models.
- Lower bounds
- Making approximative circuits exact!
- Incidence-geometry in identities.
  - Sylvester-Gallai theorems over all fields.
- Higher-dimension rank concepts.
- Duality in circuits.
  - Diagonal depth-3/4
- Bootstrapping in circuits.
- SOS (sum-of-squares) model.

Works-- Algebra inspired

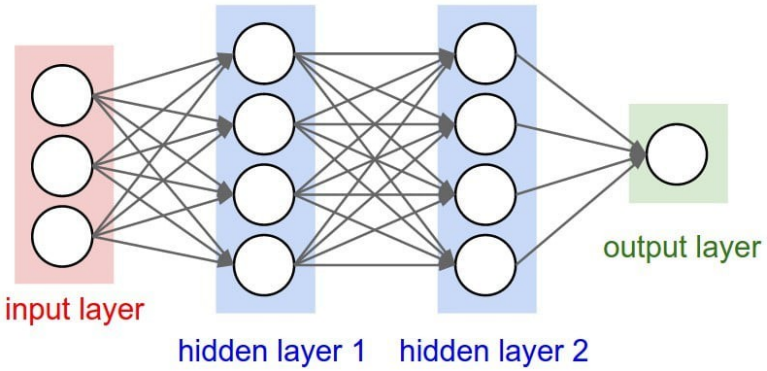
- Algebraic dependence criteria
  - The first study, over all fields.
- Factoring polynomials.
  - Circuit model
  - Sparse model
  - Mod primes
- All-roots Newton iteration
- Cubic forms equivalence
- Isomorphism problems in algebras & graphs
- Local expanders

Works-- Number theory inspired

- Primality testing
- Root-finding over p-adics
  - Or, mod prime-powers
- Igusa's local zeta function computation
- Hilbert's Nullstellensatz over Galois rings

Engineering-- Learning theory

- Areas like *Artificial Intelligence* / *Machine Learning* model decision-making using circuits.
  - Artificial Neural Networks (ANN).
- ANN is a *specialized* algebraic circuit.



- We, in CSE IITK, have started a center to solve practical problems using AI methods.
- Please see (Center for Developing Intelligent Systems) iitk.ac.in/cdis/
- cse.iitk.ac.in/users/nitin/

Thank you!