Algebra powers computation

Nitin Saxena
CSE@IITK

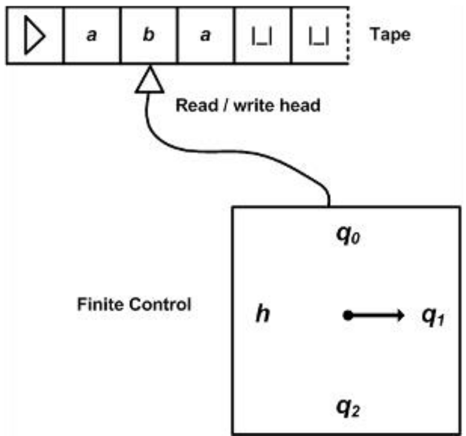
IASc Meet @ IISc Bengaluru
July 2023

What's computing?

- Alan Turing (1936) postulated a simple, most general, mathematical model for computing – Turing machine (TM).

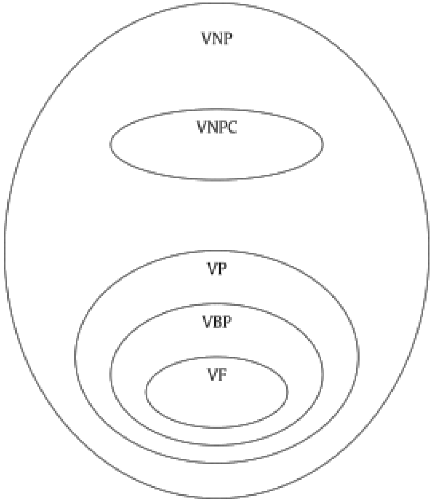
- Algorithm = TM is very much like a program.
  - TM is a real computer – highly iterative & trivial steps.

- How about an electronic circuit?
  - Algebraically, it's a neater model to capture real computation.

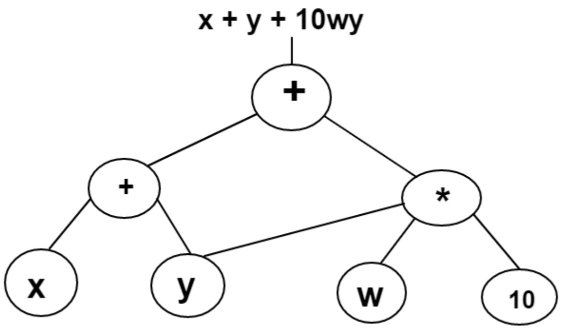


Turing (1912-1954)

Valiant: Algebraic circuits



- ❖ Valiant (1977) formalized computation & resources using algebraic circuits.
  - ➢ Giving birth to his VP ≠ VNP question.
  - ➢ Or, the algebraic hardness question!
- ❖ Algebraic circuit has constants/variables, size, depth.
- ❖ My work: Study circuit problems and their properties.
  - ➢ Develop the relevant mathematics.



Leslie Valiant (1949-)

Zero or nonzero: PIT

$$\left(a_1^2+a_2^2+a_3^2+a_4^2\right)\left(b_1^2+b_2^2+b_3^2+b_4^2\right)$$
$$=\left(a_1b_1-a_2b_2-a_3b_3-a_4b_4\right)^2+\left(a_1b_2+a_2b_1+a_3b_4-a_4b_3\right)^2$$
$$+\left(a_1b_3-a_2b_4+a_3b_1+a_4b_2\right)^2+\left(a_1b_4+a_2b_3-a_3b_2+a_4b_1\right)^2.$$

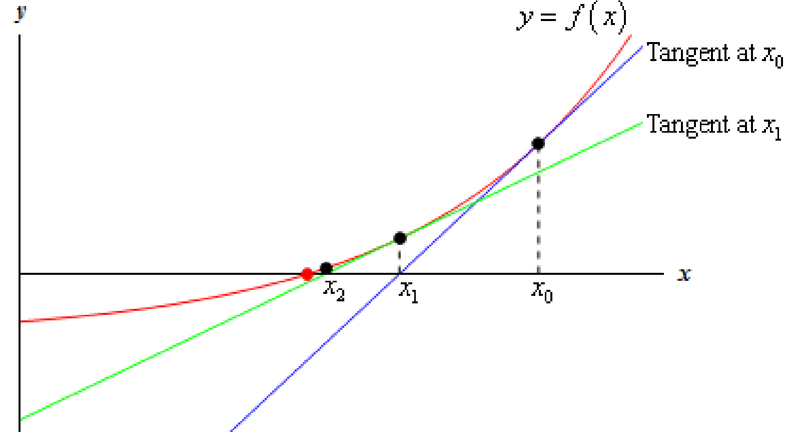
- Question: Test whether a given circuit is zero.
  - Polynomial identity testing (PIT).
- OPEN Qn: Is PIT in deterministic polynomial time?
- Motivates new tools to study algebraic computation.

- Primality testing.
- Blackbox algorithms/
  - Lower bounds (for certain models).
- Incidence-geometry in identities, over all fields.
  - Higher-dimension rank concepts.
- Duality in circuits.
  - Diagonal depth-3 or 4.
- Bootstrapping in circuits.
  - Tiny circuits
  - Sum-of-squares.

$$(X+1)^n \equiv X^n + 1 \bmod n$$

Algebraic Algorithms

Computational Algebra



- All-roots Newton iteration
  - Non-simple roots?
- Factoring polynomials.
  - Mod primes, prime-powers, p-adics
  - Circuit models
  - Approximative circuits
- Algebraic dependence criteria
- Morphism problems in algebras, graphs
- Roots counting
- Compute Zeta function analogs

$$\sqrt{2} = 3 + 1 \times 7 + 2 \times 7^2 + 6 \times 7^3 + \cdots$$

$\mathbb{Q}$–dependence of e and π ?

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "g \circ f"'] & Y \arrow[d, "g"] \\ & Z \end{tikzcd}$$

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 0$$

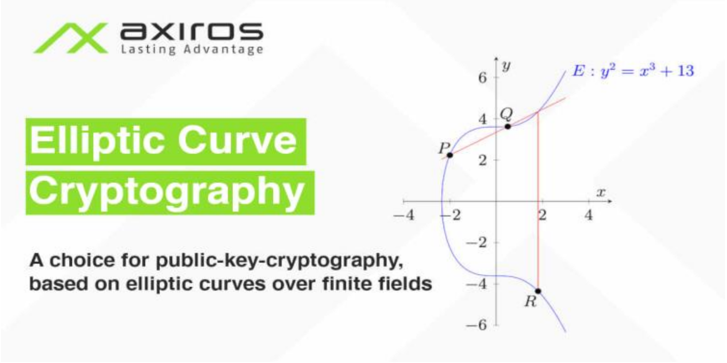
with $s \in \mathbb{C}$

Hardest question on earth since 1859.

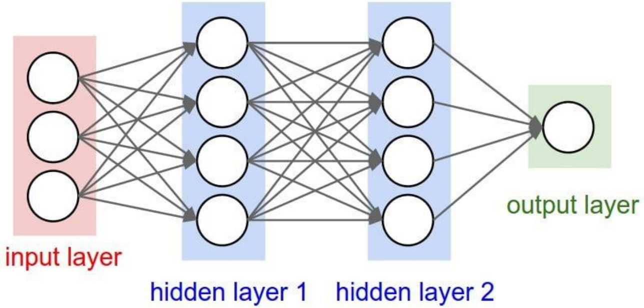
$$x = 0 = x \cdot y - 1 \text{ has } \underline{\text{root}} = (\epsilon \to 0, 1/\epsilon \to \infty)$$

Engineering

Crypto & Learning



- Cryptography uses algebra extensively.
  - Number theory, Curves, Multivariate systems
- AI/Machine Learning do decision-making using circuits.
  - Artificial Neural Networks (ANN).



- ANN is a specialized algebraic circuit.
- A Center @IITK to solve practical problems using AI methods.
- Visit (Center for Developing Intelligent Systems) www.iitk.ac.in/cdis/
  - www.cse.iitk.ac.in/users/nitin/

THANKS!