ALGEBRA POWERS COMPUTATION

Nitin Saxena
CSE@IITK
[*Thanks to the artists*]

Teacher’s Day @ IITB
September 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 computer *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.
Valiant: Algebraic circuits

- Valiant (1977) formalized computation & resources using algebraic circuits.
  - Giving birth to his $VP \neq VNP$ question.
  - Or, the algebraic hardness question!
- Algebraic circuit has constants/variables, size, depth.
**Valiant: Algebraic circuits**

- **My work:** Study circuit problems and their properties.
  - Develop the relevant mathematics.

- **De-fictionalize** the above picture!
  - Progress has been impressive.
  - Withstands AI hype.
Zero or nonzero: PIT

❖ **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.

\[
\begin{align*}
(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\
= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4)^2 + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3)^2 \\
+ (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2)^2 + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1)^2.
\end{align*}
\]

Euler’s identity (1749)

\[
\begin{align*}
10 & = 1^2 + 1^2 + 2^2 + 2^2 \\
103 & = 2^2 + 3^2 + 3^2 + 9^2 \\
312 & = 2^2 + 4^2 + 6^2 + 16^2
\end{align*}
\]

Lagrange’s four-square theorem (1770)

\[(X + 1)^n \equiv X^n + 1 \mod n \iff n \text{ is ?}
\]
Zero or Nonzero: PIT

- 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.

\[(X + 1)^n \equiv X^n + 1 \mod n\]

\[x_1, x_2, x_1^2 + x_1x_2 \text{ are dependent.}\]

\[(x_1 + \cdots + x_n)^d, \text{ as } f_1(x_1) \cdots f_n(x_n)?\]

\[f = f_1(x)^2 + \cdots + f_n(x)^2 \implies ?\]
Algebraic Algorithms
Computational Algebra

- All-roots Newton iteration
  - Non-simple roots?
  - N-variate circuit version.

- Factoring polynomials.
  - Mod primes, prime-powers, p-adics
  - Circuit models
  - Approximative circuits

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

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

But, has no actual root!
Computational Algebra

- Algebraic dependence criteria
- Morphism problems in algebras, graphs
- Roots counting
- Compute Zeta function analogs
  - Infinite information?

\[ \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 0 \quad \text{with } s \in \mathbb{C} \]

\[ P(t) := \sum_{i \geq 0} N_p^i(F)/p^{2i} \cdot t^i = \]

Is it always this simple?
Engineering
Cryptography builds on algebra.
- Number theory
- Curves, counting, morphism
- Multivariate systems

Post-quantum world requires new protocols.
- Avoid abelian groups.
- Use more complicated geometry, algebra, and lattices.

Inspiration from NP-hard problems?
- interesting beyond quantum hype
Practical Learnings

- **AI/Machine Learning**: Decision-making using circuits.  
  - Artificial Neural Networks (ANN).

- ANN is a specialized algebraic circuit.  
  - **Activation** functions are real algebraic.

- A Center @IITK to solve **practical** problems using AI methods.
  - Visit (Center for Developing Intelligent Systems)  
    [www.iitk.ac.in/cdis/](http://www.iitk.ac.in/cdis/)  
    [www.cse.iitk.ac.in/users/nitin/](http://www.cse.iitk.ac.in/users/nitin/)

Thanks!