

Polynomial Identity Testing explores if two polynomials, involving multiple variables, are equal. Algebraic methods help in determining how complicated it would be to solve this. Theoretical research in the area of Polynomial Identity Testing could potentially help in cryptography, error-correction, optimisation of algorithms and systems, and machine learning.

Algebraic circuits are used to compute polynomial equations and for Polynomial Identity Testing. A problem to be solved is represented as an algebraic circuit—a graph consisting of nodes and gates to represent inputs and operations, with directed connections between them. The number of nodes and edges represent the ‘size’ of the graph and is a representative of how long a computer could take to solve the problem.

Given a polynomial equation, one needs to find some circuit that can compute the polynomial, called upper bound problem, and also prove that a proposed circuit corresponds to the fastest way to solve it, known as the lower bound problem. “Often, this structural 'size' is more convenient to study than the sequential notion of 'time',” explains Prof. Saxena. A lower bound problem can be described as finding the smallest algebraic circuit corresponding to a polynomial.

Simple polynomial equalities, like $(X-Y)(X+Y) = X^2 - Y^2$, can be established by solving algebraically. However, when the polynomials of interest contain many variables and higher powers, the complexity increases exponentially. Finding out the exact computational complexity of Polynomial Identity Testing is one of the most important unsolved problems in this subject area. Prof. Saxena took a step forward in solving this problem through establishing that studying a very special type of circuit models would be enough to understand the properties of general circuits.

In a related study, Prof. Saxena has also developed a new framework that helped to solve another unsolved problem. He and his collaborators found a solution for Polynomial Identity Testing for the model of an algebraic circuit that has very few input variables. Here, only the inputs and outputs of a circuit are known, and the exact internal connections are not known. The proposed technique to solve this problem is likely to be useful in addressing other unsolved problems in mathematics.

The study of algebraic circuits also gives rise to new mathematical concepts. For example, Prof. Saxena has proved that the roots or solutions of specific ‘small’ circuits will be ‘small circuits’. The result is not obvious, as some small size circuits can compute very large polynomials, and the solutions of those can be large. He has also developed a new algorithm to find out whether a system of polynomial equations has a root which is very closely approximate but not exact. The new algorithm is orders of magnitude better than previous algorithms regarding computing resources and implementation time.

Prof. Saxena wishes to focus on other open problems in the area of algebraic circuits. “I would like to continue working towards strengthening the techniques and increasing their scope,” he concludes.

About :

| | |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Awardee | Prof. Nitin Saxena |
| Contact email | nitin@cse.iitk.ac.in |
| Award | Shanti Swarup Bhatnagar prize 2018 |
| Article written by | Arati Halbe |
| Image Credits | Mr. Girish Pant |
| Gubbi Labs page link | https://researchmatters.in/news/prof-nitin-saxena-iit-kanpur-awarded-shanti-swarup-bhatnagar-prize-2018-his-work-algebraic |