ARITHMETIC CIRCUIT COMPLEXITY

PROF. NITIN SAXENA
Department of Computer Science and Engineering
IIT Kanpur

TYPE OF COURSE : Rerun | Elective | UG/PG
COURSE DURATION : 12 weeks (24 Jan' 22 - 15 Apr' 22)
EXAM DATE : 23 Apr 2022

PRE-REQUISITES : Preferable (but not necessary)-- Theory of Computation, Algorithms, Algebra

INTENDED AUDIENCE : Interested students

INDUSTRIES APPLICABLE TO : Cryptography, Coding theory, Symbolic Computing Software, Learning Software

COURSE OUTLINE :

In this course we will study computation by primarily algebraic models, and use, or in many cases extend, the related tools that mathematics provides. We will start with some positive examples-- fast polynomial multiplication, matrix multiplication, determinant, matching, linear/algebraic independence, etc. The related tools are FFT (fast fourier transform), tensor rank, Newtons identity, ABP (algebraic branching program), PIT (polynomial identity testing), Wronskian, Jacobian, etc. We then move on to proofs, or attempts to prove, that certain problems are hard and impossible to express as a small circuit (i.e. hard to solve in real life too).

ABOUT INSTRUCTOR :

Prof. Nitin Saxena completed my Bachelors in Computer Science from the Indian Institute of Technology, Kanpur in 2002 and completed his PhD under Manindra Agrawal in 2006. He is broadly interested in Computational Complexity Theory, Algebra, Geometry and Number Theory. He has been a visiting graduate student in Princeton University (2003-2004) and National University of Singapore (2004-2005); a postdoc at CWI, Amsterdam (2006-2008) and a Bonn Junior Fellow (W2 Professor) at Hausdorff Center for Mathematics, Bonn (2008-2013). Since April 2013, He has a faculty position in the department of CSE, IIT Kanpur.

COURSE PLAN :

Week 1**:** Turing machines. Arithmetic circuits.

Week 2**:** Newton's identity. Arithmetic branching program. Iterated matrix multiplication.

Week 3**:** Arithmetic branching program vs. Determinant.

Week 4**:** Circuit Depth Reduction.

Week 5**:** Nontrivial reduction to constant-depth.

Week 6**:** Width reduction.

Week 7**:** Depth-3 over finite fields. Grigoriev-Karpinski measure.

Week 8**:** Raz-Yehudayoff measure for multilinear depth-3.

Week 9**:** Shifted partials of degree-restricted depth-4.

Week 10**:** Exponential lower bound for homogeneous depth-4.

Week 11**:** Polynomial Identity Testing (PIT) and exponential lower bounds are equivalent

Week 12**:** PIT for tiny depth-3 (or many other tiny models) suffices.