

Education

Dual BT-MT in Computer Science and Engineering

Kanpur, India

INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

Jul 2017 - May 2022

• M. Tech CPI - 10.0/10.0 Supervisor- Prof. Nitin Saxena

• B. Tech CPI - 9.0/10.0

Research Interests

COMPUTATIONAL COMPLEXITY THEORY, COMPUTATIONAL ALGEBRA, PSEUDORANDOMNESS, ERROR CORRECTING CODES

Publications

1. On algorithms to find p-ordering



- Aditya Gulati, Sayak Chakrabarti, Rajat Mittal
- 7th Annual Conference on Algorithms and Discrete Applied Mathematics (CALDAM), 2021
- submitted to the special issue of Discrete Applied Mathematics dedicated to CALDAM 2021

2. Graphon Estimation from Partially Observed Network Data



• Soumendu Sundar Mukherjee, Sayak Chakrabarti

• submitted to the Journal of Computational and Graphical Statistics (JCGS) [under major revision]

Research Experience

Roots of multivariate polynomials modulo powers of large primes [M. TECH THESIS]



PROF. NITIN SAXENA, IIT KANPUR

Jul 2020- Present • Working on an algorithm to find roots of degree- $d\ n$ -variate polynomials modulo prime powers for constant d and n

- Applied techniques to lift roots of multivariate polynomials from finite fields \mathbb{F}_p to p-adic fields
- · Learnt about techniques from computational algebra including multivariate Taylor's expansion, resultants etc.
- · Studied algebraic geometry, with a focus on complexity of Hilbert's Nullstellensatz, dimension of variety, algebraic set decomposition etc.

Root sets and p-ordering



PROF. RAJAT MITTAL, IIT KANPUR

Jun 2020 - Sep 2021

- · Worked on solving linear inequalities in integers and optimizing to find a polynomial representing the root set
- Studied about p-ordering, root sets of polynomials, their properties and methods to calculate the number of root sets $mod p^k$
- Attempted to use representative roots and p-ordering to check if a given set is a valid root set
- Devised an efficient algorithm to find p-ordering of integers and root sets in $\mathbb{Z}/p^k\mathbb{Z}$ given in succinct representations

Designer Commutative Algebra

PROF. PETTERI KASKI, AALTO UNIVERSITY

Apr 2021 - Present

- Studied multivariate batch evaluation, multivariate interpolation, sparse polynomial arithmetic, Gröbner basis etc.
- Experimented with some ideals to find a ring extension followed by a substitution for faster multivariate polynomial evaluation
- Currently analyzing existing results and attempting to find faster methods of multivariate evaluation by studying ring extensions and homomorphisms

Continuous Skolem Problem for higher dimensions



PROF. JÖEL OUAKNINE, DR. ENGEL LEFAUCHEUX, DR. EIKE NEUMANN, MPI-SWS

May 2020 - Jul 2020

- Attempted to prove the decidability of zeroes of exponential polynomials for low codimension cases using semi-algebraic sets and their decomposition
- Studied the work done upto dimension 8 and attempted to extend it using Schanuel's conjecture and Leon Ehrenpreis' conjecture
- Devised a parameterization of a semi-algebraic set which contains the zeroes of the given function

Factorization of polynomials modulo prime powers



PROF. RAJAT MITTAL, IIT KANPUR

Aug 2019-Jun 2020

- Worked on finding factorization techniques to return a factorization of polynomials with maximum number of linear factors $\bmod p^k$
- · Learnt about algorithms on factorization of polynomials in finite fields and methods to lift them to modulo prime powers
- Studied representative roots, root-finding modulo prime powers, Newton polygons etc.
- Gave a result for degree 3 polynomials to show that linear factors correspond to different representative roots

Graphon Estimation from Partially Observed Network Data



PROF. SOUMENDU SUNDAR MUKHERJEE, ISI KOLKATA

Dec 2018 - Dec 2020

- Learnt about graphons and their estimation methods including universal singular value thresholding, stochastic blockmodel approximation, matrix completion, neighborhood smoothing etc.
- Extended the neighborhood smoothing technique to give an algorithm to estimate the underlying graphon on partially revealed graphs
- Estimated graphons using various existing alternative methods and compared those against the proposed algorithm on simulated and real networks

Linear Cryptanalysis Applied to Logic Locking



1

PROF. PRAMOD SUBRAMANYAN, IIT KANPUR

May 2019 - Oct 2019

· Learnt about Logic Locking and tested linear cryptanalysis applied to various benchmark circuits

Teaching Experience

Tutor, ESC101: Fundamentals of Computing

INSTRUCTORS: PROF. SWARNENDU BISWAS AND PROF. HAMIM ZAFAR, IIT KANPUR

Oct 2021 - Present

· Conducted weekly tutorial sessions, helped with setting questions for quizzes and labs, graded labs and exams

Teaching Assistant, CS203: Probability for Computer Science

INSTRUCTOR: PROF. NITIN SAXENA, IIT KANPUR

Mar 2021 - May 2021

• Conducted tutorial sessions, graded exams and assignments

Teaching Assistant, CS202: Logic for Computer Science

INSTRUCTOR: PROF. SUNIL SIMON, IIT KANPUR

Jan 2021 - Feb 2021

· Graded exams

Volunteer, Shiksha Sopan

SOPAN SCHOOL

Apr 2019 - Mar 2020

- · Volunteered with Shiksha Sopan, an NGO aimed at providing education to economically weaker section of the society
- Conducted weekly English Grammar classes to children of classes 6-8

Academic Mentor, MTH101: Single Variable Calculus & MTH102: Linear Algebra and ODEs

COUNSELLING SERVICES, IIT KANPUR

Aug 2018 - Apr 2019

· Helped students facing academic problems in mathematics by conducting remedial classes and one-to-one mentorship

Talks & Presentations

Quantum Information Theory and Applications to Local Decoding

Apr 2021

Towards Mordell's Theorem: A Useful Homomorphism

P

COURSE: ARITHMETIC GEOMETRY

COURSE: OUANTUM COMPUTING

Nov 2020

Weierstrass Normal Form Course: Arithmetic Geometry Oct 2020

Factorization of polynomials modulo prime powers

Undergraduate Project

Jul 2020

Honors & Awards

2	2020	Research Fellow, Max Planck Institute of Software Systems
	2017	All India Rank- 181, Joint Entrance Exam, Advanced, among 200,000 candidates
	2017	All India Rank- 287, Joint Entrance Exam, Main, among 1.2 million candidates
	2017	State Rank-10, West Bengal Joint Entrance Exam, among 150,000 candidates
	2017	Qualified Indian National Physics Olympiad (INPhO), among top 34 students selected from India
	2016	Qualified Indian National Mathematical Olympiad (INMO), among top 30 students selected from India
	2015	All India Rank- 115, Kishore Vaigyanik Protsahan Yojana, among 100,000 candidates

Other Professional Activities

Sub-Reviewer | Journal of Number Theory

Aug 2021 - Sep 2021

• Sub-reviewed a paper for Journal of Number Theory under the guidance of and edited by Prof. Nitin Saxena

Project Mentor Association for Computing Activities

Jan 2019 - Apr 2019

• Guided a group of first year students in topics of Theoretical Computer Science

Jul 2018 - Apr 2019

· Provided emotional and academic assistance to 4 freshmen and helped them adjust to campus environment

Graduate Courses

Student Guide | Counselling Service

Randomized Methods in Computational Complexity, Algebraic Number Theory, Computational Number Theory and Algebra, Geometric Topology, Modern Cryptology, Arithmetic Geometry,

Quantum Computing, Algorithmic Information Theory, Computational Complexity Theory*

* - ongoing course

2

Skills

Programming Python, C/C++, R, SageMath, Haskell

Libraries Qiskit, Pytorch, Tensorflow, Numpy, Keras, OpenCV