

Sayak Chakrabarti

☎ (+91) 8777582670 | ✉ sayaksc@gmail.com | 🌐 sayaksc.github.io | 📄 sayaksc

Education

Dual BT-MT in Computer Science and Engineering

INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

Kanpur, India

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
- 7-th 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

Root-finding algorithms for multivariate polynomials modulo prime-powers [M. TECH

THESIS]

PROF. NITIN SAXENA, IIT KANPUR

Jul 2020- Present

In this thesis, we explore algorithms to find roots of multivariate polynomials modulo powers of primes. The idea is to lift each root in \mathbb{F}_p step by step to p -adics. In the beginning, I learnt about polynomial factorization, root counting and algebraic geometry, a report of which is available. We attempted to fix roots at each step and lift to the next step. However, since roots at each step can affect the existence of roots in the following steps, we are forming ideals in $\mathbb{Z}_p[\bar{x}]$ to satisfy the properties of these roots. Currently, we are focussing on bivariate, as the techniques used translate to multivariate as well. Once this ideal is formed, we can solve them using methods from [HW99]. The draft of this project is under preparation.

Designer Commutative Algebra

PROF. PETTERI KASKI, AALTO UNIVERSITY

Apr 2021 - Present

In this project, we are currently looking for ways to find faster algorithms for multivariate batch evaluation. The idea was motivated from [KU08]. We intended to construct a ring extension by taking modulo an ideal followed by substitution of variables to evaluate the polynomial. I learnt about several techniques using computer algebra and ideals, and we used these to construct the ideal. We axiomatized the properties that need to be satisfied in order to give an intuition on the structure of the ideal we need to form. In this process, we are currently exploring ideals to satisfy the properties.

Root sets and p -ordering

PROF. RAJAT MITTAL, IIT KANPUR

Jun 2020 - Sep 2021

We attempted to give an algorithm to decide if a given subset of $\mathbb{Z}/p^k\mathbb{Z}$ is a valid root set. We studied properties of root sets, its connections to p -ordering and methods of counting root sets. We reduced this problem of deciding root sets to inequalities having some non-linear terms in order to construct a polynomial corresponding to the root set. We are currently working on solving the system of inequalities by iteratively finding the values. In doing this, we required computing p -ordering of roots given in succinct representations using representative roots. The research led to a paper that finds p -ordering of subsets of integers as well as on sets given in succinct form.

Continuous Skolem Problem for higher dimensions

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

May 2020 - Jul 2020

Our goal was to determine the decidability of zeroes of exponential polynomials. We attempted to extend the existing work using Schanuel's conjecture and Leon Ehrenpreis' conjecture to higher dimensions. Semi-algebraic sets and their decompositions were used in our approach. We attempted to find a polynomial lower bound of a set representing the zero set. In this process, we gave a parameterization of the set and extended a proposition to continuously extend bounded continuous semialgebraic functions to $\bar{0}$.

Factorization of polynomials modulo prime powers

PROF. RAJAT MITTAL, IIT KANPUR

Aug 2019-Jun 2020

The problem of factorization of polynomial modulo prime powers was the focus of this project. We worked on returning a factorization into maximum number of linear factors, and studying the properties of such factors using representative roots and p -ordering. I learnt about several techniques used in factorization of polynomials in fields and rings. Based on our study, we proved a property that gave a factorization algorithm for cubic polynomials modulo p^k using representative roots.

Graphon Estimation from Partially Observed Network Data

PROF. SOUMENDU SUNDAR MUKHERJEE, ISI KOLKATA

Dec 2018 - Dec 2020

We worked on estimating network edge probabilities seen as graphons. This project started with reviewing literature on existing graphon estimation techniques and finding possibilities to extend them. Based on neighborhood smoothing technique, we gave an algorithm called neighborhood smoothing extended that returned probability estimations of edges of partially revealed graphs. We compared our method against some existing methods in simulated graphons and real data, and our algorithm worked better in most.

Linear Cryptanalysis Applied to Logic Locking

PROF. PRAMOD SUBRAMANYAN, IIT KANPUR

May 2019 - Oct 2019

We applied an idea based on linear cryptanalysis in an attempt to break logic locking encryptions. Here, I learnt about existing attacks on logic locking, and tested our approach on small 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



COURSE: QUANTUM COMPUTING

Apr 2021

Towards Mordell's Theorem: A Useful Homomorphism



COURSE: ARITHMETIC GEOMETRY

Nov 2020

Weierstrass Normal Form



COURSE: ARITHMETIC GEOMETRY

Oct 2020

Factorization of polynomials modulo prime powers



UNDERGRADUATE PROJECT

Jul 2020

Honors & Awards

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

Student Guide | COUNSELLING SERVICE

Jul 2018 - Apr 2019

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

Graduate Courses

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

Skills

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

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