

# Mudit Aggarwal

mudit19063@iiitd.ac.in | +91-9910679251 | v1ator.github.io

## EDUCATION

**INDRAPRASTHA INSTITUTE OF INFORMATION TECHNOLOGY**  
BACHELOR OF TECHNOLOGY | COMPUTER SCIENCE AND ENGINEERING

**NEW DELHI, INDIA**  
EXPECTED MAY 2023

- Cumulative GPA: 9.18/10
- Received Dean's Award for Academic Excellence

## PUBLICATIONS AND PREPRINTS

- [1] Mudit Aggarwal and T Aaron Gulliver. A New Self-Shrinking Generator (submitted). 2022. URL: <https://www.researchsquare.com/article/rs-2348688/v1>, doi:10.21203/rs.3.rs-2348688/v1.
- [2] Mudit Aggarwal and Samrith Ram. Generating Functions for Straight Polyomino Tilings of Narrow Rectangles. *J. Integer Seq.*, 26(1):Art. 23.1.4, 12, 2023. URL: <https://cs.uwaterloo.ca/journals/JIS/VOL26/Ram/ram3.pdf>.

## RESEARCH EXPERIENCE

### REED SOLOMON CODES AND THEIR VARIANTS | Undergraduate Thesis

ADVISOR: DR. ANURADHA SHARMA  
August 2022 - Present

IIIT DELHI, INDIA

- Working on generalising and finding variants to Reed-Solomon Codes, particularly **Twisted RS Codes**, that can be used to detect and correct **Insertion-Deletion errors** during transmission.
- Aiming to use the variants being developed to give error correcting codes for **DNA Sequences**.
- Using techniques from **Algebraic Coding Theory**, as well as Combinatorics, Finite Fields, Number Theory, Modern Algebra, and Linear Algebra.

### GENERATING FUNCTIONS FOR TILING RECTANGLES

ADVISOR: DR. SAMRITH RAM  
May 2021 - November 2022

IIIT DELHI, INDIA

- Worked on finding **multivariate generating functions** for the number of ways to tile an  $m \times n$  rectangle with an unlimited number of  $k \times 1$  and  $k \times k$  tiles, allowing for free rotations.
- Also worked on finding the generating functions for the number of tilings with constraints on the number of tiles.
- Using topics and techniques from **Combinatorics**, **Generating Functions**, **Recurrences**, and **Number Theory**.
- A paper [2] has been published in the Journal of Integer Sequences.

### SHRINKING GENERATORS FOR CRYPTOGRAPHY | Mitacs Globalink Research Internship

ADVISOR: DR. AARON GULLIVER  
May 2022 - November 2022

UNIVERSITY OF VICTORIA, CANADA

- Worked on finding new **Self-Shrinking Generators** for cryptography, while also generalising the notion of **LFSRs** by introducing **non-linearities** in them. This ensures **better security guarantees** in both theory and practice.
- Compared multiple types of such generators like LFSRs, Cellular Automata, Shrinking Generators, Modified Generators, etc. Additionally, analysing the security of these both **theoretically** as well as **practically**.
- A paper [1] has been submitted and is currently under review.

### BOUNDED ARBORICITY GRAPH STREAMING

ADVISORS: DR. SAKET SAURABH & DR. AKANKSHA AGRAWAL  
Jan 2021 - May 2021

IMSc CHENNAI & IIT MADRAS, INDIA  
(Remote)

- Worked with Sameep Dahal, Savit Gupta, and Agastya Vibhuti Jha on finding **small-space approximation algorithms** for graphs with a given bounded arboricity, in the streaming model.
- Proved results and small-space algorithms for **Vertex Cover**, **b-Matching**, and **Capacitative Matching** for weighted graphs under the streaming model, and unweighted graphs under the dynamic model.

### SUNFLOWER LEMMA AND LIFTING THEOREMS

ADVISOR: DR. SAJIN KOROTH  
May 2022 - September 2022

UNIVERSITY OF VICTORIA, CANADA

- Worked on improving the **gadget-size** guarantees of **lifting theorems** in communication complexity using the recent improvements in the **Erdos-Rado Sunflower Lemma**.

- Conversely, also used **randomised lifting theorems** and **decision tree complexity** to further the lower bounds on the size in the sunflower lemma.

## WORKSHOPS

### ALGORITHMS FOR BIG DATA AND ML | ACM WINTER SCHOOL 2020-21

Institute of Mathematical Sciences, Chennai

- The workshop was organised by **Dr. Saket Saurabh** and **Dr. Venkatesh Raman** on **Streaming Algorithms**.
- The main topics covered were: Chernoff bounds, Morris counter, Lower Bounds, AMS estimator, Sparse recovery, Johnson–Lindenstrauss lemma, Graph streaming and PAC learning.

### ALGORITHMS AND LOWER BOUNDS | ACM WINTER SCHOOL 2021-22

IIT Madras and CMI, Chennai

- The workshop was organised by **Dr. Akanksha Agrawal** and **Dr. G. Philip** on **Algorithmic Lower Bounds**.
- The main topics covered were: Fast Fourier Transform, Linear Decision Trees, Polynomial Methods, Complexity Conjectures, and Reductions.

## RELEVANT COURSEWORK

### GRADUATE

Functional Analysis (A) [Class Rank 1]

Abstract Algebra II (A)

Calculus on  $\mathbb{R}^n$  (A)

Approximation Algorithms (A)

Theory of Modern Cryptography (A)

Topics in Number Theory (B)

Applied Cryptography (B-)

Measure and Probability Theory

Information Theory

Randomised Algorithms

Lattices in Computer Science

Algebraic Coding Theory \*

Quantum Computing \*

Communication Complexity \*

### UNDERGRADUATE

Discrete Maths (A+) [Class Rank 1]

Real Analysis II (A) [Class Rank 1]

Abstract Algebra I (A)

Probability and Statistics (A)

Differential Equations (A)

Theory of Computation (A)

Data Structures and Algorithms (A)

Linear Algebra (A-)

Real Analysis I (A-)

Analysis & Design of Algorithms (A-)

Basic Electronics (A-)

Modern Algorithm Design (B)

Signals and Systems (B)

Combinatorics and Applications \*

Multivariate Calculus \*

Number Theory \*

\*Course audited with instructor's permission

### READING COURSES

#### COMBINATORICS AND REPRESENTATION THEORY (A)

Advisor: Dr. Samrith Ram

Monsoon Semester, 2022

- Studied an assortment of topics from **Combinatorics** and **Representation Theory**, using multiple texts.
- Main topics covered were Snake Oil, WZ Pairs, Gosper's Algorithm, Pólya-Redfield Theorem, Cycle Index, Symmetric Functions, Partitions, Weighted Objects, and Tableaux.
- Some texts used were *Generatingfunctionology* by Wilf, *A = B* by Zeilberger, Wilf, Petkovšek, *A Course in Enumeration* by Aigner, and *Bijjective Combinatorics* by Loehr.

#### DIFFERENTIAL GEOMETRY WITH TOPOLOGY (A)

Advisor: Dr. Shilpak Banerjee

Summer Semester, 2021

- Studied **Point-Set Topology** from *Topology* by Munkres.
- Covered sections on **Differential Geometry** from *Elementary Differential Geometry* by Pressley.
- Also covered the required multivariable calculus and multivariable analysis prerequisites.
- Main topics included: Topology, Basis for topology, Metric Spaces, Connectedness, Compactness, Homeomorphisms, Curves and Surfaces, Parameterisations and Reparameterisations, Manifolds, Orientability of Surfaces, and Isometries.

#### ADVANCED LINEAR ALGEBRA \*

Advisor: Dr. Samrith Ram

Winter Semester, 2022

- Studied **Linear Algebra** from *Linear Algebra* by Hoffman & Kunze, and *Linear Algebra Done Right* by Axler.
- Main topics included: Vector Spaces, Basis, Fields, Matrix Systems, Dual Spaces, Functionals, Cyclic Decompositions, Jordan Form, Canonical Forms, and Inner Product Spaces.

### TEACHING ASSISTANTSHIPS

Functional Analysis ● Combinatorics and Applications ● Discrete Mathematics ● Abstract Algebra I ● Multivariate Calculus

## PROGRAMMING PROJECTS & SKILLS

### QUADROTOR DRONE SIMULATOR

Cyborg: Robotics Club at IIITD

April 2020 - June 2020



- Created a quadrotor simulator in Python that takes quadrotor size, dynamics, and path points as input.
- Uses **Euler-Newtonian** rigid body dynamics, and a multi-loop **PID** controller to simulate the motion of the given quadrotor and give plots for the motion of the same, along with graphs of the errors.

### COLOUR SWITCH

Advanced Programming: Course Project

Monsoon Semester, 2020



**PROFICIENT IN:** SageMath ● Julia ● LaTeX ● Beamer ● Python ● C++ ● C ● Java