

# Mudit Aggarwal

muditagg@student.ubc.ca | v1ator.github.io

## EDUCATION

### THE UNIVERSITY OF BRITISH COLUMBIA

MASTER OF SCIENCE | MATHEMATICS

- Advisor: Dr. Andrew Rechnitzer
- Cumulative Percentage: 86.3/100

VANCOUVER, CANADA

2023 - PRESENT

### INDRAPRASTHA INSTITUTE OF INFORMATION TECHNOLOGY

BACHELOR OF TECHNOLOGY | COMPUTER SCIENCE AND ENGINEERING

- Cumulative GPA: 9.21/10
- Received Dean's Award for Academic Excellence

NEW DELHI, INDIA

2019-2023

## PUBLICATIONS AND PREPRINTS

- [1] **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.
- [2] **Mudit Aggarwal** and T Aaron Gulliver. A New Self-Shrinking Generator (submitted to *J. Cryptogr. Eng.*). 2022.

## RESEARCH EXPERIENCE

### GENERATING FUNCTIONS FOR TILING RECTANGLES

ADVISOR: DR. SAMRITH RAM

IIIT DELHI, INDIA

May 2021 - November 2022

- 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.
- A paper [1] has been published in the Journal of Integer Sequences.

### INTERACTIVE CAPACITY OF A BINARY ERASURE CHANNEL

ADVISOR: DR. MANUJ MUKHERJEE

IIIT DELHI, INDIA

March 2023 - Present

- Working on improving the lower bounds for the interactive capacity of a noisy binary erasure channel.
- Provided an updated coding scheme and a new way of error analysis of protocols using Markov Chains to model error patterns for stochastic errors.
- A manuscript is currently being written.

### RANDOM WALKS ON SCHREIER COSET GRAPHS

ADVISOR: DR. ANDREW RECHNITZER

UBC, CANADA

September 2023 - Present

- Working on asymptotics of generating functions arising from random walks on Schreier Coset Graphs.

### REED SOLOMON CODES AND THEIR VARIANTS | Undergraduate Thesis (A)

ADVISOR: DR. ANURADHA SHARMA

IIIT DELHI, INDIA

August 2022 - May 2023

- Worked 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.
- Additionally, worked on finding MDS and LCD codes, useful in preventing side-channel and fault injection attacks using Orthogonal Direct-Sum masking.

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

ADVISOR: DR. AARON GULLIVER

UVic, CANADA

May 2022 - November 2022

- 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, analyzing the security of these both **theoretically** as well as **practically**.

- A paper [2] 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 **Capacitive 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 **randomized lifting theorems** and **decision tree complexity** to further the lower bounds on the size in the sunflower lemma.

## WORKSHOPS

### SIGNAL PROCESSING, COMMUNICATIONS AND NETWORKS | JTG/IEEE SUMMER SCHOOL 2023

Indian Institute of Science, Bengaluru

- The speakers were **Dr. Gautam Kamath**, **Dr. Nilanjana Datta**, and **Dr. Rashmi Vinayak**.
- The talks included Differential Privacy, Quantum Information Theory, quantum data compression, quantum state discrimination, manipulation of entanglement, and Coding Theory for Distributed Systems.

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

Institute of Mathematical Sciences, Chennai (online)

- The speakers were **Dr. Saket Saurabh**, **Dr. Venkatesh Raman**, and **Dr. Fahad Panolan**.
- The main topics covered were: Streaming Algorithms, Chernoff bounds, Morris counter, Lower Bounds, AMS estimator, Sparse recovery, Johnson-Lindenstrauss lemma, Graph streaming and PAC learning.

## COURSEWORK (AT UBC)

Measure Theory and Integration (A)

Probability Theory (A)

Fields and Galois Theory (A)

Topology (A-)

Discrete Maths

Compressed Sensing

Functional Analysis \*

Complex Analysis \*

Real Variables 2 \*

Math Teaching Techniques

Representations of Finite Groups (Reading Seminar)

Discrete Math and Discrete Geometry (Reading Seminar)

## COURSEWORK (AT IIITD)

### GRADUATE

Information Theory (A+)

Functional Analysis (A)

Randomised Algorithms (A)

Abstract Algebra II (A)

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

Approximation Algorithms (A)

Theory of Modern Cryptography (A)

Lattices in Computer Science (A-)

Topics in Number Theory (B)

Applied Cryptography (B-)

Measure and Probability Theory \*

Algebraic Coding Theory \*

Communication Complexity \*

### UNDERGRADUATE

Discrete Maths (A+)

Real Analysis II (A)

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-)

Modern Algorithm Design (B)

Signals and Systems (B)

Combinatorics and Applications \*

Multivariate Calculus \*

Number Theory \*

Fields and Waves \*

### TEACHING ASSISTANTSHIPS

Combinatorics and Applications

2x Abstract Algebra

Discrete Mathematics

Multivariate Calculus

### READING COURSES

Combinatorics and Representation Theory (A)

Topology and Differential Geometry (A)

Probabilistic Method in Combinatorics \*

Advanced Linear Algebra \*

Spectral and Algebraic Graph Theory \*

Information Theory and Combinatorics \*

\*Course audited or sat through.