Photo: AboveSummit and Christopher Harting

Ninth Annual Conference

May 2019

Ninth Annual PRIMES Conference

May 18–19, 2019

Saturday, May 18

8:45 am Welcoming Remarks

- Prof. Michel Goemans, Head of the MIT Mathematics Department
- Prof. Pavel Etingof, PRIMES Chief Research Advisor
- Dr. Slava Gerovitch, PRIMES Program Director

9:15 am Session 1: Fractals and Visualization Algorithms

- Jason Liu, *Approximating the dimension of circle packings*
  (mentor Prof. Sergiy Merenkov, CCNY – CUNY)
- Oliver Hayman, *Analyzing visualization and dimensionality-reduction algorithms*
  (mentor Ashwin Narayan)
- Ziyan (Heidi) Lei, *Fractals: Hausdorff dimension, the Koch curve, and visibility*
  (mentor Dr. Tanya Khovanova)

10:15 am Session 2: Applied Mathematics

- Tejas Gopalakrishna, *Analysis of the one line factoring algorithm on large semiprimes*
  (mentor Yichi Zhang)
- Yizhen Chen, *Mobile sensor networks: Bounds on capacity & complexity of realizability*
  (mentor Dr. Jesse Geneson, Iowa State)
- Sanjit Bhat, *Probing the structure of deep neural networks with universal adversarial perturbations* (mentor Dimitris Tsipras)

11:15 am Session 3: Geometry and Topology

- Zander Hill, *On the distortion of torus knots* (mentor Luis Kumanduri)
- Nithin Kavi, *Cutting and gluing surfaces* (mentor Zhenkun Li)
- Srinivasan Sathiamurthy, *Critical lattices of symmetric convex domains*
  (mentor Anurag Rao, Brandeis University)

12:00 pm Lunch in Honor of PRIMES head mentor Dr. Tanya Khovanova's 60th birthday

1:30 pm Session 4: Combinatorics

- Sebastian Jeon, *3-symmetric graphs* (mentor Dr. Tanya Khovanova)
- Lucy Cai, Espen Slettnes, and Jeremy Zhou, *Extracting tree-statistics from the quasisymmetric Bernardi polynomial* (mentor Duncan Levear, Brandeis University)

2:35 pm Session 5: Algebra

- Rupert Li, *Compatible recurrent identities of the sandpile group and maximal stable configurations* (mentor Yibo Gao)
- Victor Luo and Sasha Shashkov (reading group), *Introduction to representation theory* (mentor Yau Wing Li)
- Elias Sink and Allen Wang (reading group), *Character theory of finite groups* (mentor Christopher Ryba)

3:40 pm Session 6: Algebraic Geometry and Representation Theory

- Lev Kruglyak, *The rational Cherednik algebra of type* A_1 *with divided powers in characteristic* p (mentor Daniil Kalinov)
- Frank Wang, *The shuffle algebra of the Hilbert scheme of the plane* (mentor Yu Zhao)
- Arav Karighattam, *The Galois group of the 27 lines on a rational cubic surface* (mentor Yongyi Chen)
- Brandon Wang, *Quotients of tropical moduli spaces* (mentor Dr. Dhruv Ranganathan, University of Cambridge)

4:50 pm Session 7: PRIMES Circle

- Peter Haine, PRIMES Circle Coordinator, *Introduction*
- Tal Berdichevsky and Corinne Mulvey, *Graph theory and map coloring* (mentor Agustin García)
- Ishita Goluguri and Christina Li, *Burnside's lemma: A combinatorial application of group actions* (mentor Maya Sankar)
- Hanfei Cui and Trisha Lahiry, *Multiplicity, convolution, and the Möbius inversion formula* (mentor Michael Tang)

Sunday, May 19

8:45 am Welcoming Remarks

- Dr. Slava Gerovitch, PRIMES Program Director
- Dr. Tanya Khovanova, PRIMES Head Mentor

9:00 am Session 8: Combinatorics

- Ezra Erives, *Mixed strategy equilibria for winner takes all variant of Colonel Blotto* (mentor Dr. Zarathustra Brady)
- Kevin Wu, *On base 3/2 and greedy partitioning of integers* (mentor Dr. Tanya Khovanova)
- Isha Agarwal, Paul Braverman, Patrick Chen, William Du, Kaylee Ji, Akhil Kammila, Shane Lee, Alicia Li, Anish Mudide, Jeffrey Shi, Maya Smith, and Isabel Tu (PRIMES STEP Junior group), *Weighing coins, losing weight, and saving money* (mentor Dr. Tanya Khovanova)
- Matvey Borodin, Aidan Duncan, Joshua Guo, Kunal Kapoor, Anuj Sakarda, Jerry Tan, Armaan Tipirneni, Max Xu, and Kevin Zhao (PRIMES STEP Senior group), *Common knowledge: Games of logic* (mentor Dr. Tanya Khovanova)

10:20 am Session 9: Combinatorics

- Benjamin Wright, *Maximal extensions of differential posets* (mentor Christian Gaetz)
- Christopher Zhu, *Enumerating permutations with singleton double descent sets* (mentor Pakawut Jiradilok)
- Justin Yu, *On subset sums and thin additive bases* (mentor Dr. Asaf Ferber)
- Andrew Weinfeld, *Bases for quotients of symmetric polynomials* (mentor Guangyi Yue)

11:30 am Session 10: Applied Mathematics

- Janabel Xia, *Sampling over tilings of the plane: A computational approach against political gerrymandering* (mentor Younhun Kim)
- Benjamin Kang, *All-pay auctions with different forfeit functions* (mentor Prof. James Unwin, University of Illinois at Chicago)
- Yuyuan Luo, *Minimal percolating sets with time-dependent bootstrap percolation* (mentor Prof. Laura Schaposnik, University of Illinois at Chicago)
- Victoria Zhang, *Patterns and symmetries in networks of spiking neurons* (mentor Dr. Bolun Chen, Brandeis University)
- Sunay Joshi, *On the degenerate Turán problem and its variants* (mentor Dr. Zilin Jiang)

1:30 pm Session 11: PRIMES Circle

- Peter Haine, PRIMES Circle Coordinator, *Introduction*
- Sofia Mrowka, Elizabeth Zhong, and Natasa Zupanski, *Game theory: A playful presentation* (mentor Marisa Gaetz)
- Michelle Li and Ella Serrano-Wu, *Solving problems in combinatorics using induction and generating functions* (mentor Uma Roy)
- Ai-Wen Joy Lim and Eve Martin, *The Application of knot theory to models in statistical mechanics* (mentor Radha Mastandrea)
- Ildi Hoxhallari and Brian Kubinec, *Probability, discrete distributions and Markov chains* (mentor Daniel León Jiménez)

3:00 pm Session 12: Computer Science

- Prof. Srini Devadas, Department of Electrical Engineering and Computer Science, *Welcoming Remarks*
- David Lu, *Group messaging in the XRD private communication system* (mentor Albert Kwon)
- Shashvat Srivastava, *AnonStake: An anonymous proof-of-stake cryptocurrency via zero-knowledge proofs and Algorand* (mentor Kyle Hogan)
- Robert Chen, *Scalable distributed key generation* (mentor Alin Tomescu)
- Yiming Zheng, *Vector commitments from univariate polynomials and their applications* (mentor Alin Tomescu)
- John Kuszmaul, *Verkle trees: Ver(y short Mer)kle trees* (mentor Alin Tomescu)

SATURDAY, MAY 18

SESSION 1: FRACTALS AND VISUALIZATION ALGORITHMS

Jason Liu

Approximating the dimension of circle packings

Mentor: Prof. Sergiy Merenkov, CCNY – CUNY

Project suggested by Prof. Sergiy Merenkov, CCNY – CUNY

This project examines the dimension of the residual sets of round packings, and attempts to determine the validity of a question from Chris Bishop that the Apollonian Gasket has the lowest Hausdorff dimension of all residual sets of round packings. The residual sets of round packings are found by removing a collection of open, disjoint, round disks from the plane. Our hope is that numerical estimates for the dimensions of the residual sets of various round packings will either provide strong evidence for the positive answer to Bishop's question or that we will find an example with a strictly smaller dimension.

Oliver Hayman

Analyzing visualization and dimensionality-reduction algorithms

Mentor: Ashwin Narayan

Project suggested by Ashwin Narayan

In order to visualize high dimensional data sets, scientists use mapping algorithms to map high dimensional data to low dimensional data sets that are easy to visualize. The most prominent of these algorithms is the t-Stochastic Neighbor Embedding algorithm, abbreviated as t-SNE. This talk will describe a metric created to evaluate the clustering of data sets and how a parameter of the t-SNE algorithm affects the clustering of the data sets it outputs, as evaluated by this metric. We will introduce methods for generalizing the behaviour of this metric for uniform distributions in different dimensions and the behaviour of the data sets t-SNE outputs.

Ziyan (Heidi) Lei

Fractals: Hausdorff dimension, the Koch curve, and visibility

Mentor: Dr. Tanya Khovanova

Project suggested by Prof. Larry Guth

The Koch curve is an iteratively constructed fractal with Hausdorff dimension $\log_3 4$. We are interested in calculating the Hausdorff dimension of the visible portion of the Koch curve viewed from various points of visibility. In this presentation, we define the concept of point visibility, motivate the definition of Hausdorff dimension, and present

our results in determining the Hausdorff dimension of the Koch curve from points of visibility in certain regions of the plane.

SESSION 2: APPLIED MATHEMATICS

Tejas Gopalakrishna

Analysis of the one line factoring algorithm on large semiprimes

Mentor: Yichi Zhang

Project suggested by Dr. Stefan Wehmeier, Mathworks

We look at the One Line Factoring Algorithm. We first observe which values are returned by the algorithm while factoring semiprimes pq, and the numbers for which the algorithm is efficient. We also look at how the algorithm efficiency is affected when we change the iterator k of the algorithm.

Yizhen Chen

Mobile sensor networks: Bounds on capacity & complexity of realizability

Mentor: Dr. Jesse Geneson, Iowa State

Project suggested by Dr. Jesse Geneson, Iowa State

We study the models, proposed by Chen Gu et al. in 2018, of mobile sensor networks where the sensors receive information continuously and can store an infinite amount of information. Their paper proposed two models—the combinatorial mobile sensor network (CMSN) where each time exactly two sensors communicate, and the geometric mobile sensor network (GMSN) where the sensors move in constant speed on a line—and a way to measure the capacity of a network to diffuse information. We found the maximum and minimum capacities of GMSNs, a restricted form of CMSN (RCMSN) where every two sensors communicate exactly once, and restricted GMSNs (RGMSNs) where there is only a limited number of distinct speeds of sensors. We also found that the problem of determining if an RCMSN is equivalent to a GMSN is NP-hard, and whether a CMSN is equivalent to an RGMSN with 3 distinct speeds can be determined in polynomial time.

Sanjit Bhat

Probing the structure of deep neural networks with universal adversarial perturbations

Mentor: Dimitris Tsipras

Project suggested by Sanjit Bhat

In recent years, it has been shown that Deep Neural Networks (DNNs) are susceptible to adversarial examples, small input perturbations that fool the network into predicting the wrong class. While regular adversarial examples are specially crafted for a particular image (i.e., image-specific), Universal Adversarial Perturbations (UAPs) are single perturbations that fool a classifier across most images from a particular class (i.e., class-specific). Since UAPs by definition generalize to several images, we view them as a lens through which to understand the more general dynamics of DNNs. Specifically, we show a connection between robustness to adversarial examples and changes in the loss landscape and classification strategies of neural networks.

SESSION 3: GEOMETRY AND TOPOLOGY

Zander Hill

On the distortion of torus knots

Mentor: Luis Kumanduri

Project suggested by Prof. Larry Guth

We show that for sufficiently large q, the distortion of $T_{p,q}$ is bounded above by $\frac{7q}{\log q}$.

Nithin Kavi

Cutting and gluing surfaces

Mentor: Zhenkun Li

Project suggested by Zhenkun Li

We start with a disk with $2n$ vertices along its boundary where pairs of vertices are connected with n strips with certain restrictions. This forms a *pairing*. For a given pairing, we show that cut and glue operations do not change an invariant known as the *signature.* Pairings with a signature of 0 are special because they can be transformed into closed surfaces through cut and glue operations that have other applications in topology. We prove that all balanced pairings for a fixed n are connected.

Srinivasan Sathiamurthy

Critical lattices of symmetric convex domains

Mentor: Anurag Rao, Brandeis University

Project suggested by Prof. Dmitry Kleinbock, Brandeis University

Given a symmetric convex domain K in $\mathbb{R}^2$, we study its admissible lattices. These are the lattices which intersect the interior of K trivially. Out of all admissible lattices, we study the critical set of those lattices which have the smallest covolume. Given any compact set $C \subset \mathbb{R}$, we construct a domain which has a critical set homeomorphic to C. We also state the connection of this problem to lattice packings.

SESSION 4: COMBINATORICS

Sebastian Jeon

3-symmetric graphs

Mentor: Dr. Tanya Khovanova

Project suggested by Dr. Tanya Khovanova

An intuitive property of a random graph is that its subgraphs should also appear randomly distributed. We consider graphs whose subgraph densities exactly match their expected values. Starting from 74 such graphs on 8 vertices, we discuss constructing larger graphs both theoretically and with the aid of a computer.

Lucy Cai, Espen Slettnes, and Jeremy Zhou

Extracting tree-statistics from the quasisymmetric Bernardi polynomial

Mentor: Duncan Levear, Brandeis University

Project suggested by Prof. Olivier Bernardi, Brandeis University

The Tutte polynomial is an extensively studied polynomial invariant of graphs. Awan and Bernardi defined the Bernardi polyomial, a trivariate polynomial invariant on digraphs, and showed that, up to a change in variables, it extends the Tutte polynomial to digraphs. Further, they defined a generalization of the Bernardi polynomial, called the quasisymmetric Bernardi polynomial (QSBP), a formal power series in an infinite number of variables that extends the Tutte symmetric function to digraphs.

A question of interest is what information the QSBP provides about the underlying digraph. The Tutte symmetric function does not uniquely distinguish all graphs, so the QSBP cannot distinguish all digraphs; in other words, there exist non-isomorphic graphs that share the same QSBP.

Three decades ago, Stanley posed a question equivalent to "Does the Tutte symmetric function distinguish trees?" We study the information that can be extracted from the QSBP on rooted trees, with the aim of determining whether or not QSBPs are unique on rooted trees. We show that a rooted-tree-statistic we name the "co-height profile profile" is extractable, and that the QSBP distinguishes rooted 2-caterpillars.

SESSION 5: ALGEBRA

Rupert Li

Compatible recurrent identities of the sandpile group and maximal stable configurations

Mentor: Yibo Gao

Project suggested by Prof. David Perkinson, Reed College

In the abelian sandpile model, recurrent chip configurations are of interest as they are a natural choice of coset representatives under the quotient of the reduced Laplacian. In this talk, we investigate graphs whose recurrent identities with respect to different sinks are compatible with each other. The maximal stable configuration is the simplest recurrent chip configuration, and graphs whose recurrent identities equal the maximal stable configuration are of particular interest, and are said to have the complete maximal identity property. We prove that given any graph G one can attach trees to the vertices of G to yield a graph with the complete maximal identity property. We conclude with several intriguing conjectures about the complete maximal identity property of various graph products.

Victor Luo and Sasha Shashkov

Introduction to representation theory

Mentor: Yau Wing Li

Reading group

For any group, let a *representation* of that group be a correspondence of each group element with a linear transformation in an n-dimensional vector space (over any field).

The representation theory of finite groups studies properties of and categorizes the representations of a group. In this talk, we will discover a few introductory results in representation theory—we will learn how to classify the entire set of representations of any finite group using its *irreducible* representations, and we will introduce the concept of a representation's *character*.

Elias Sink and Allen Wang

Character theory of finite groups

Mentor: Christopher Ryba

Reading group

Often when we study an abstract algebraic structure, we may represent each of the elements as matrices acting on a vector space. This allows us to work with the structure in a familiar linear algebraic setting. In this talk, we study the representation theory of finite groups using characters. Although characters, defined by traces of matrices, do not seem particularly enlightening at first, several powerful results related to their orthogonality give a concise way of understanding and manipulating the representations of a group.

SESSION 6: ALGEBRAIC GEOMETRY AND REPRESENTATION THEORY

Lev Kruglyak

The rational Cherednik algebra of type A_1 with divided powers in characteristic p

Mentor: Daniil Kalinov

Project suggested by Prof. Pavel Etingof

We study the rational Cherednik algebra of type A_1 (where $t = 1$), its spherical subalgebra, and its maximal divided power extensions in characteristic p. We derive p-adic valuation formulas for powers of Dunkl operators, as well as symmetrized and antisymmetrized powers of Dunkl operators. Using these, we compute a list of generators for divided power extensions of both algebras. Finally, we provide abstract definitions of the constructed divided power extensions and conjecture about their equivalence to the combinatorial definitions.

Frank Wang

The shuffle algebra of the Hilbert scheme of the plane

Mentor: Yu Zhao

Project suggested by Yu Zhao

We examine the shuffle algebra over the ring $\mathbf{R} = \mathbb{C}[q_1^{\pm 1}, q_2^{\pm 1}]$, which was found by Schiffmann and Vasserot to act on the equivariant K-theory of the Hilbert Scheme of points in the plane. We find that the modules of 2 and 3 variable elements of the shuffle algebra are finitely generated, and prove a necessary condition for an element to be in the shuffle algebra for arbitrarily many variables.

Arav Karighattam

The Galois group of the 27 lines on a rational cubic surface

Mentor: Yongyi Chen

Project suggested by Prof. Joe Harris, Harvard University

For any rational cubic surface, consider the minimal field extension of the rationals over which all of the 27 lines on the surface are defined. In our project, we investigate which Galois groups may occur in this way; these are subgroups of the Weyl group of E_6. One method of constructing cubic surfaces is by blowing up the plane at six points, and defining the associated generators as the coordinates of the rational map from the plane to its blow-up. In this talk we will describe properties of the Galois group in the case that the generators are all rational, or that the six points lie in Galois orbits, and mention examples of cubic surfaces without rational generators.

Brandon Wang

Quotients of tropical moduli spaces

Mentor: Dr. Dhruv Ranganathan, University of Cambridge

Project suggested by Dr. Dhruv Ranganathan, University of Cambridge

We will provide an overview of algebraic geometry and various algorithms for taking the tropicalization of an affine variety. We then introduce the moduli space $\mathcal{M}_{0,n}$ and $\mathcal{M}(\vec{x})$ and their tropicalizations. Finally, we discuss the fan structure of $\mathcal{M}_{0,n}^{\text{trop}}$ and $\mathcal{M}(\vec{x})^{\text{trop}}$ and current progress on the investigations of the Chow quotient of $\mathcal{M}(\vec{x})$.

SESSION 7: PRIMES CIRCLE

Tal Berdichevsky and Corinne Mulvey

Graph theory and map coloring

Mentor: Agustin García

We discuss the foundations of graph theory and how common types of graphs and their properties can be used to model various scenarios such as group of Facebook friends and a group of Fakebook enemies. Using the properties of these common types of graphs, we will prove several theorems relating to the planarity of graphs. Planarity is the property which allows a graph to be drawn so that no two lines cross. We then apply the properties of planar graphs and introduce the idea of coloring to solve a problem involving the minimum number of colors which can be used to color the regions of a map.

Ishita Goluguri and Christina Li

Burnside's lemma: A combinatorial application of group actions

Mentor: Maya Sankar

Group actions can be applied in many fascinating ways in group theory. One of these applications is Burnside's lemma, which allows us to count the number of objects up to certain symmetries, like rotation. In this talk, we present a few combinatorial applications of Burnside's lemma, namely, counting the colorings of different geometric patterns up

to rotation/reflection and counting the arrangements of colored beads on a necklace. We prove the lemma by using a myriad of important tools from group theory.

Hanfei Cui and Trisha Lahiry

Multiplicity, convolution, and the Möbius inversion formula

Mentor: Michael Tang

Our talk will focus on three functions of number theory, the multiplicity function, convolution, and the Möbius inversion formula. In the multiplicity function section, we will define the function, and showcase some important multiplicative functions for counting divisors of an integer. In the convolution section, we will provide the definition of convolution, prove the commutative and multiplicative properties of convolution, prove how to construct multiplicative functions using convolution, and prove using convolution the multiplicativity of the functions showcased in the multiplicity section. In the Möbius inversion formula section, we will define the Möbius μ-function, prove the identity function for the Möbius inversion formula, and define and prove the Möbius inversion formula and its converse using convolution.

SUNDAY, MAY 19

SESSION 8: COMBINATORICS

Ezra Erives

Mixed strategy equilibria for winner takes all variant of Colonel Blotto

Mentor: Dr. Zarathustra Brady

Project suggested by Dr. Zarathustra Brady

Colonel Blotto is a well-studied family of games where two generals simultaneously split their armies across several battlefronts, trying to maximize the expected number (or total weight) of the battles they win. We study a variant of this game in which the generals instead try to maximize their probabilities of winning a majority of the battles. We show that optimal strategies for the standard Colonel Blotto game do not perform well in the winner-takes-all variant, and prove the existence of Nash equilibria for the latter. Finally, we numerically compute Nash equilibria for a discretization of the problem.

Kevin Wu

On base 3/2 and greedy partitioning of integers

Mentor: Dr. Tanya Khovanova

Project suggested by Dr. Tanya Khovanova

We discuss the connection between fractional base $\frac{3}{2}$ and greedy partitioning of integers into sequences that do not contain arithmetic progression. On the way, we put numbers into a table with fractal properties.

Isha Agarwal, Paul Braverman, Patrick Chen, William Du, Kaylee Ji, Akhil Kammila, Shane Lee, Alicia Li, Anish Mudide, Jeffrey Shi, Maya Smith, and Isabel Tu
(PRIMES STEP Junior group)

Weighing coins, losing weight, and saving money

Mentor: Dr. Tanya Khovanova

Project suggested by Dr. Tanya Khovanova

We study a problem that involves using a balance scale to determine if bags of coins are labeled correctly. We find the combinations that either use the least coins or have the least weight. So, join us to find out how to lose weight and save money at the same time!

Matvey Borodin, Aidan Duncan, Joshua Guo, Kunal Kapoor, Anuj Sakarda, Jerry Tan, Armaan Tipirneni, Max Xu, and Kevin Zhao (PRIMES STEP Senior group)

Common knowledge: Games of logic

Mentor: Dr. Tanya Khovanova

Project suggested by Dr. Tanya Khovanova

We discuss several logic games played by infinitely intelligent sages where each sage tries to figure out the color of their hat or the number on their forehead. The difficult question is what everyone knows about what everyone knows about what everyone knows...

SESSION 9: COMBINATORICS

Benjamin Wright

Maximal extensions of differential posets

Mentor: Christian Gaetz

Project suggested by Christian Gaetz

Byrnes proved that the Fibonacci poset realizes the largest possible rank sizes for a differential poset. We expand on his work by proving that the Fibonacci poset is the *unique* largest one. This poset is constructed from repeated iterations of reflection-extension; in the future we hope to show that the reflection-extension construction is a maximal extension for any partial differential poset.

Christopher Zhu

Enumerating permutations with singleton double descent sets

Mentor: Pakawut Jiradilok

Project suggested by Pakawut Jiradilok, Dr. Tanya Khovanova, and Dr. Claude Eicher

Denote by $dd(I;n)$ the number of permutations $w \in \mathfrak{S}_n$ with double descent set I. In this paper, we discuss the enumeration of permutations for given I, specifically singleton sets I. We present a recursive formula for $dd(I;n)$ and a method to estimate values of $dd(I;n)$ both for singleton I. Additionally, we discuss related combinatorial objects, circular permutations and rim hooks, which allow us to characterize double descents in other ways. Finally, we end with a few conjectures.

Justin Yu

On subset sums and thin additive bases

Mentor: Dr. Asaf Ferber

Project suggested by Dr. Asaf Ferber

An additive basis of order k is a set $B \subset \mathbb{N}$ such that every positive integer n can be written as a sum of at most k possibly overlapping elements of B. A classical result of Erdős established the existence of an additive basis of order 2 for which no number n is represented $\Theta(\log n)$ times. Such bases are called thin. In this talk, extending a later result of Erdős and Tetali, we investigate the existence of thin bases of order k which can grow with n.

Andrew Weinfeld

Bases for quotients of symmetric polynomials

Mentor: Guangyi Yue

Project suggested by Prof. Darij Grinberg, University of Minnesota at Minneapolis

Two constructs in algebraic geometry are well known to be isomorphic to quotients involving symmetric polynomials and ideals generated by complete homogeneous symmetric polynomials. In the process of producing this isomorphism, a basis for these quotients is described in terms of the Schur polynomials. Grinberg recently showed that the same basis holds across a family of quotients. We have examined a variation using the power sum symmetric polynomials in place of the complete homogeneous symmetric polynomials.

SESSION 10: APPLIED MATHEMATICS

Janabel Xia

Sampling over tilings of the plane: A computational approach against political gerrymandering

Mentor: Younhun Kim

Project suggested by Prof. Moon Duchin, Tufts University, and Younhun Kim

In the political scene, the boundaries of electoral districts can be rigged to favor one party over another in a process called gerrymandering. This problem is easy to see when irregular, non-"compact" district shapes show up. To simplify, we model the problem of electoral districting through tilings of a grid of cells. We wish to be able to algorithmically sample from the set of tilings uniformly at random, which will also allow us to determine "fairness" of an existing tiling. A natural method is to use Markov chains. In this talk, we first describe our proposed Markov chain and introduce basic Markov chain theory along the way. We make conjectures about some combinatorial properties of our state space (of tilings) that would reveal effectiveness of our Markov chain. The main end goal is to be able to weigh our Markov chain to have a stationary distribution that favors "compact" tilings.

Benjamin Kang

All-pay auctions with different forfeit functions

Mentor: Prof. James Unwin, University of Illinois at Chicago

Project suggested by Prof. James Unwin, University of Illinois at Chicago

A common method of selling items is via auction. In an auction, each bidder bids a certain amount of money, and the bidder bidding the most is the winner. The amount of money each bidder must pay is variable depending on the type of auction. These auctions can also be used as a model for other real world conflicts. We focus on all-pay auctions and extend existing result in the literature for a generalized forfeit function. I will also outline out future intentions to investigate results of auctions with more forms of the forfeit function, different natures of bidders, and more prizes. These results would allow sellers to know the optimal auction in which to sell items and tell bidders the optimal bid they should make.

Yuyuan Luo

Minimal percolating sets with time-dependent bootstrap percolation

Mentor: Prof. Laura Schaposnik, University of Illinois at Chicago

Project suggested by Prof. Laura Schaposnik, University of Illinois at Chicago

r-Bootstrap percolation describes a deterministic process where vertices of a graph are infected once r neighbors of it are infected. We generalize this to a time-dependent process, where a vertex is infected if a "percolation function" $F(t)$ number of its neighbors are infected at time t. An initial set of infected vertices is a percolating set if it infects all vertices at a finite time; moreover, it is a minimal percolating set if no proper subsets of it percolate. We describe a polynomial-timed algorithm to find one smallest minimal percolating set on finite trees for certain $F(t)$-bootstrap percolation models.

Victoria Zhang

Patterns and symmetries in networks of spiking neurons

Mentor: Dr. Bolun Chen, Brandeis University

Project suggested by Dr. Bolun Chen, Brandeis University

The human brain, composed of 100 billion neural cells, is one of the most complex systems in nature. To understand brain functions such as perception or motor-control, we study neural models of spiking neurons — specifically the integrate and fire model. In this talk, we examine the dynamics of a small system of pulsed-coupled integrate and fire neurons. In particular, we aim to understand the conditions necessary for different dynamical solutions to arise. We consider symmetry within a network and employ both numerical and analytical techniques in our analysis of two-cell and three-cell neural networks.

Sunay Joshi

On the degenerate Turán problem and its variants

Mentor: Dr. Zilin Jiang

Project suggested by Dr. Zilin Jiang

Given a family of graphs $\mathcal{F}$, a central problem in extremal graph theory is to determine the maximum number $\text{ex}(n, \mathcal{F})$ of edges in a graph on n vertices that does not contain any member of $\mathcal{F}$ as a subgraph. The *degenerate Turán problem* considers the asymptotic behavior of $\text{ex}(n, \mathcal{F})$ for familes $\mathcal{F}$ of bipartite graphs. In this talk, we discuss several notions central to providing lower bounds on extremal numbers, including balanced rooted graphs and the Erdős–Simonovits Reduction Theorem. In addition, we present new lower bounds on the asymmetric extremal number $\text{ex}(m, n, F)$ of blowups of bipartite graphs and of theta graphs.

SESSION 11: PRIMES CIRCLE

Sofia Mrowka, Elizabeth Zhong, and Natasa Zupanski

Game theory: A playful presentation

Mentor: Marisa Gaetz

In this talk, we explore both combinatorial and classical game theory. Combinatorial game theory is the study of games like Chess or Checkers, where two players alternate turns until one wins the game. Classical game theory studies games like Rock Paper Scissors, where each player simultaneously makes a single decision without knowing the decision of the other player. We will focus on the basic definitions and terms of game theory by diving deeper into two original games: Roads and One Four All. After covering basic concepts, we will discuss the combinatorial side of game theory with Roads, and will conclude by discussing the classical side with One Four All.

Michelle Li and Ella Serrano-Wu

Solving problems in combinatorics using induction and generating functions

Mentor: Uma Roy

Induction is an extremely simple but powerful mathematical proof technique used to solve a wide variety of combinatorial problems. Induction is generally used to show that a certain property holds for all natural numbers $n \in \mathbb{N}$. First one shows the property holds for $n = 1$, and then shows if it holds for arbitrary k, then the property also holds for $k+1$. A particular class of problems that are solvable by induction is providing closed form solutions for sequences defined by recurrences. However, another mathematical technique known as generating functions sometimes proves more adept at solving these classes of problems, although they are more complex to use. In this talk, we will explore the broad class of problems of providing closed form formulae for sequences, and show how induction and generating functions can both be used to solve them.

Ai-Wen Joy Lim and Eve Martin

The Application of knot theory to models in statistical mechanics

Mentor: Radha Mastandrea

In this talk, we begin by explaining some basic knot theory terminology by walking through a few problems. We then discuss the applications of knot theory to statistical mechanics, exploring the use of Ising models to represent interactions between particles. We discuss the mathematical results of these Ising models, specifically the Yang-Baxter equation, to help us develop more complex models. We then examine how the connection between this relation and Reidemeister moves in knot theory can allow us to strengthen these models.

Ildi Hoxhallari and Brian Kubinec

Probability, discrete distributions and Markov chains

Mentor: Daniel León Jiménez

In our talk, we will examine some important counting and probability principles. We will also present some discrete random variable distributions: Bernoulli, binomial, and geometric, and illustrate how binomials could be approximated using Poisson random variables. Finally, we will quickly analyze and exemplify the concept of Markov chains.

Session 12: Computer Science

David Lu

Group messaging in the XRD private communication system

Mentor: Albert Kwon

Project suggested by Albert Kwon

XRD (short for Crossroads) is a metadata private messaging system that uses multiple mix networks to provide cryptographic privacy, while scaling easily to support more users by adding more servers. In this work, we investigate ways to modify XRD to allow for group messaging in addition to one-to-one messaging. We try several approaches, including greedy algorithms, linear programming, and mixed-integer programming. Our results show that for 100 servers and 1 million users, XRD can support up to 5-person conversations with the cost of 96% increased latency. The same network can support up to 25-person conversations while incurring 250% greater latency.

Shashvat Srivastava

AnonStake: An anonymous proof-of-stake cryptocurrency via zero-knowledge proofs and Algorand

Mentor: Kyle Hogan

Project suggested by Kyle Hogan

We present AnonStake, the first anonymous Proof-of-Stake cryptocurrency. AnonStake builds on Algorand, a Proof-of-Stake cryptocurrency that features fast block times and

consensus. The anonymous transactions are based on ZeroCash, an anonymous cryptocurrency that uses zero-knowledge proofs to hide transaction details. In Algorand consensus, users are selected to form committees at rates proportional to their wealth. Traditionally, users need to know each other's account balances to verify that committees were formed properly. We construct a zero-knowledge proof that allows users to participate in Algorand consensus without revealing their identity or their wealth, thus preserving privacy. The construction uses new cryptographic primitives, such as MiMC, that are designed for applications in zero-knowledge proofs.

Robert Chen

Scalable distributed key generation

Mentor: Alin Tomescu

Project suggested by Alin Tomescu

A (t, n)-distributed key generation (DKG) protocol allows n players to jointly generate a public and secret key such that no one knows the secret key but any set of t players can reconstruct it. DKGs are an integral component of distributed protocols, such as threshold signature schemes, random beacons, and proactive secret sharing schemes. Yet existing DKG protocols do not scale beyond tens of thousands of players without requiring prohibitive amounts of computation. In this work, we present new techniques that drastically reduce computation in DKG protocols from quadratic to quasilinear time. The net result is a DKG protocol that can scale to hundreds of thousands of players and could enable new distributed applications on a scale never seen before.

Yiming Zheng

Vector commitments from univariate polynomials and their applications

Mentor: Alin Tomescu

Project suggested by Alin Tomescu

Vector Commitment (VC) schemes are a key component of stateless cryptocurrencies. In this work, we present a novel vector commitment scheme from univariate polynomials. Like previous schemes, our scheme supports efficiently updating the VC and all of its proofs after an update. However, unlike previous VC schemes, our scheme supports efficiently precomputing all proofs in quasilinear time. Furthermore, due to our use of univariate polynomials, our scheme has useful algebraic structure. Thanks to these two key properties, our scheme can not only be applied to stateless cryptocurrencies, but can also help scale Verifiable Secret Sharing (VSS) protocols and Distributed Key Generation (DKG) protocols.

John Kuszmaul

Verkle trees: Ver(y short Mer)kle trees

Mentor: Alin Tomescu

Project suggested by Alin Tomescu

We introduce Verkle Hash Trees (VHTs), a bandwidth-efficient flavor of Merkle Hash Trees (MHTs). Verkle trees offer proof sizes that are ten times smaller than in MHTs, at

the cost extra computation. Despite their higher computation, Verkle trees can still support thousands of appends per second, making them very useful for reducing bandwidth in public-key directories. We prove the viability of this approach by implementing our construction in C++.