Photo: Slava Gerovitch

Twelfth Annual Spring-Term PRIMES Conference

May 21-22, 2022

2022 PRIMES Spring Term Conference

Saturday, May 21

Mathematics

10:00 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

10:15-11:15 am: Session 1. PRIMES Circle

Crystal Egbunike & Wintana Tewolde, “Graph Theory and Its Applications” (mentor Victor Chu)
Pete Olhava & Alexander Gil Osorio, “An Introduction to Knot Theory” (mentor Preston Cranford)
Sebastian Cuervo & Ben Stokes, “Triangles in Various Geometries” (mentor Paige Dote)

11:25 am-12:45 pm: Session 2. PRIMES Circle

Ling (Esther) Fu & Sarah Pan, “The Busy Beaver Problem” (mentor Alexandra Hoey)
Jessica Guo & Audrey Wei, “NP-Completeness” (mentor Kerri Lu)
Zoe Awa & Ankita Varigonda, “Game Theory” (mentor Yuyuan Luo)
Elena Baskakova & Alice He, “Probability Theory: Why You Are Falsely Convicted, Lonely, and in Debt” (mentor Jeremy Smithline)

1:45-2:45 pm: Session 3. PRIMES Circle

Maya Koreth & Dania Rustom, “Number Theory and Divisibility Issues” (mentor Ariana Park)
Sophia Hou & Jaeyi Song, “Group Theory” (mentor Merrick Cai)
Gracie Sheng & Evelyn Zhu, “Symmetry and Simplicity in Finite Group Theory” (mentor Gabrielle Kaili-May Liu)

3:00-3:40 pm: Session 4. PRIMES STEP

Hwiseo Choi, Shreyas Ekanathan, Aidan Gao, Sylvia Zia Lee, Rajarshi Mandal, Vaibhav Rastogi, Daniel Sheffield, Michael Yang, Angela Zhao, and Corey Zhao (PRIMES STEP Junior group), “The Struggles of Chessland” (mentor Dr. Tanya Khovanova)
Eric Chen, Adam Ge, Andrew Kalashnikov, Ella Kim, Evin Liang, Mira Lubashev, Matthew Qian, Rohith Raghavan, Benjamin Taycher, Samuel Wang (PRIMES STEP Senior group), “Disarray in the Tribarray: A Tribsploration” (mentor Dr. Tanya Khovanova)

4:00-4:55 pm: Session 5. Math Reading Groups

Anuj Sakarda and Jerry Tan, “The Probabilistic Method” (mentor YounHun Kim)
Yi (Alex) Liang, “Representation Theory and Quantum Systems” (mentor Sanjay Raman)
Ilaria Seidel, Nathan Xiong, and William Yue, “Dynkin Quivers and Their Representations” (mentor Dr. Aleksandra Utiralova)

Sunday, May 22

Mathematics

10:00 am: Welcoming Remarks

Prof. Pavel Etingof, PRIMES Chief Research Advisor
Dr. Slava Gerovitch, PRIMES Program Director

10:10-10:45 am: Session 6. Math Reading Groups

Joshua Guo, Andrew Lee, and Karthik Seetharaman, “Galois Theory and the Insolvability of the Quintic” (mentor Chun Hong Lo)
Kevin Zhao, “Lie Matrices” (mentor Sanjay Raman)

10:55-11:50 am: Session 7. PRIMES Circle

Leisha Fortunat, “A Simple Introduction to Graph Theory” (mentor Rachana Madhukara)
Daniela Yablon & Ayelet Yablon, “Introduction to Cryptography” (mentor Aparna Gupte)
Zoe Siegelnickel & Palak Yadav, “Algorithm Analysis” (mentor John Shackleton)

Computer Science and Computational Biology

1:00 pm: Welcoming Remarks

Prof. Srini Devadas, PRIMES Computer Science Section Coordinator

1:05-2:05 pm: Session 8. Computer Science

Rachel Chen, “Uotchi: A Hardware Platform to Create and Exchange Non Fungible Objects” (mentor Jules Drean)
Abigail Thomas, “The Implementation of Model Pruning to Optimize zk-SNARKs in Machine Learning” (mentor Yu Xia)
Tanisha Saxena, “A Systematic Study on the Difference and Conversion Between Synchronous and Asynchronous Protocols” (mentor Jun Wan)
Zifan (Carl) Guo, “Understanding High-Level Properties of Low-Level Programs through Transformers” (mentor William Moses)

2:15-2:45 pm: Session 9. Computer Science and Computational Biology

Kevin Edward Zhao, “Life after BERT: What Do Other Muppets Understand about Language?” (mentors Prof. Anna Rumshisky and Vladislav Lialin, UMass Lowell)
Neil Chowdhury, “A Mechanism of Formation for a Unique Compartment in the Silkworm Genome” (mentor Sameer Abraham)

2022 PRIMES CONFERENCE ABSTRACTS

SATURDAY, MAY 21

SESSION 1: PRIMES CIRCLE

Crystal Egbunike & Wintana Tewolde

Graph Theory and Its Applications

Mentor: Victor Chu

At its simplest, graph theory is the study of graphs as a mathematical object. While it may be hard to recognize, graph theory can be used to solve many problems in the real world. One example is finding the shortest path between two locations on a map. The Dijkstra Algorithm, which finds the shortest path from a 'source node' or vertex to another vertex in the graph, can solve this problem. Another example is building a search engine that can display the web pages in the order of relevance and importance to the user's query. PageRank was Google's solution for this problem, and it also heavily relies on graph theory. In our presentation, we will discuss the different aspects of graph theory that are applied to Dijkstra Algorithm and PageRank.

Pete Olhava & Alexander Gil Osorio

An Introduction to Knot Theory

Mentor: Preston Cranford

Knot theory is a subfield of topology. In this talk, we briefly discuss the basic concepts of knot theory. This includes the definitions of knots, the three Reidemeister moves, and planar isotopy. In addition to these topics, we will also elaborate on knot invariants, and tricolorability. Then we show how Reidemeister moves preserve tricolorability. After this, we talk about applying knot theory to biology using DNA and topoisomerases.

Sebastian Cuervo & Ben Stokes

Triangles in Various Geometries

Mentor: Paige Dote

This talk is an exploration of the ways that one of the most useful shapes in Euclidean geometry—triangles—generalizes to different, and in some ways more philosophic, geometries. This extends from the introduction of axiomatic systems, building into initial constructions of triangles in both spherical and hyperbolic spaces to the history behind their discovery, ending in an examination of single elliptic geometry.

Ling (Esther) Fu & Sarah Pan

The Busy Beaver Problem

Mentor: Alexandra Hoey

First introduced in 1962 by mathematician Tibor Radó, the busy beaver problem asks for an upper bound on the number of operations a computer with certain limitations can perform. Since then, researchers have shown that knowing certain values of the busy beaver function would reduce determining the truth or falsity of various long-standing conjectures to finite-step computations. In our presentation, we will discuss topics in computability theory including Turing machines, decidability, and the halting problem. Our talk will culminate in a proof that one cannot computationally solve the busy beaver problem, as well as a brief discussion of its implications for other fields of mathematics.

Jessica Guo & Audrey Wei

NP-Completeness

Mentor: Kerri Lu

We study the fundamentals of time complexity in computational complexity theory. We discuss polynomial time and nondeterministic polynomial time. We consider NP-complete problems, the hardest problems in NP, which hold importance in the work on the P vs. NP problem.

Zoe Awa & Ankita Varigonda

Game Theory

Mentor: Yuyuan Luo

We will be exploring combinatorial games, a branch of game theory, which allows us to understand the topic of decision-making and uses simple games to work out different strategies that result in various outcomes. Game theory is based on the heuristic of rational thinking where a player makes decisions that benefit them optimally based on the outcomes it brings them. This method of thinking can be applied to larger fields such as economics and finance for parties to maximize their own income. In our talk, we will analyze the partisan game Hackenbush and its applications.

Elena Baskakova & Alice He

Probability Theory: Why You Are Falsely Convicted, Lonely, and in Debt

Mentor: Jeremy Smithline

Probability theory has many interesting and engaging problems. We cover several of these problems and explore the underlying ideas. After an introduction to basic probability through the Birthday problem, we discuss dependency, conditional probability, and Bayes' formula, using the prosecutor's fallacy to demonstrate a common misconception regarding conditional probability in a real-world context. We will also touch on the mathematics behind the friendship paradox and why this seemingly unfounded phenomenon exists, focusing on the topics of random variables, expected values, and variance. Finally, we will delve into Markov chains and steady states through the gambler's ruin problem, explaining why it is probably not a good idea to gamble if you wish to stay out of debt.

SESSION 3: PRIMES CIRCLE

Maya Koreth & Dania Rustom

Number Theory and Divisibility Issues

Mentor: Ariana Park

In this talk, we introduce important topics in elementary number theory, with a special focus on divisibility and congruence relations. Using these ideas, we define the Euclidean algorithm, modular arithmetic, and primitive roots and apply these concepts through multiple problems, including a proof of Lagrange's four square theorem.

Sophia Hou & Jaeyi Song

Group Theory

Mentor: Merrick Cai

In our presentation, we will give an introduction to group theory with an emphasis on group presentations (via generators and relations). Group theory is a part of abstract algebra and it is the study of groups, which are sets under binary operations that satisfy specific conditions. We will go over some examples and non examples of groups, as well as homomorphisms. Then, we will apply this to two fun and interesting problems in group theory, which address fields and generators and relations.

Gracie Sheng & Evelyn Zhu

Symmetry and Simplicity in Finite Group Theory

Mentor: Gabrielle Kaili-May Liu

In this talk, we explore notable properties of symmetric groups followed by a discussion of their subgroup structure and Cayley table. In addition, we note the appearance of permutation and symmetry in nature and in real-world applications. We further examine finite simple groups, which arise from the decomposition of groups into normal subgroups and a quotient group. Finite simple groups are isomorphic to cyclic groups of prime order, alternating groups, groups of Lie type, and sporadic groups. We study the construction of such groups and identify patterns and symmetries in their subgroup lattices.

SESSION 4: PRIMES STEP

Hwiseo Choi, Shreyas Ekanathan, Aidan Gao, Sylvia Zia Lee, Rajarshi Mandal, Vaibhav Rastogi, Daniel Sheffield, Michael Yang, Angela Zhao, and Corey Zhao (PRIMES STEP Junior group)

The Struggles of Chessland

Mentor: Dr. Tanya Khovanova

In this talk, we introduce Chessland, a magical kingdom of chess pieces, hidden away in a large archipelago of the Bermuda Triangle. We discuss the surveying of Chessland where the King, the Queen, and their escorts—the Rook, the Bishop, and the Knight—go on a journey to see every square county on each of their square checkerboard-like islands of many different sizes. We calculate how long it takes each member to survey their given island. Unexpectedly, during their journeys, the forces identify an enemy invasion in their surveying and move to trap these enemy forces. Sometimes they succeed, and sometimes they find themselves at a stalemate.

Eric Chen, Adam Ge, Andrew Kalashnikov, Ella Kim, Evin Liang, Mira Lubashev, Matthew Qian, Rohith Raghavan, Benjamin Taycher, Samuel Wang (PRIMES STEP Senior group)

Disarray in the Tribarray: A Tribsploration

Mentor: Dr. Tanya Khovanova

Do you want to be prepared for life or death temperature conversions? Then head on over to our talk, where we will teach you a TRIBck to use! Using our revolutionary techniques, we extend properties of the well-known Fibonacci sequence to the lesser-known Tribonacci sequence. We explore Tribonacci representations of natural numbers, a maTRIBx of Tribonacci-like sequences, and many of this maTRIBx's unique atTRIButes such as the descriptions of some columns and how to estimate any term. Come for the life or death situations, and stay for the TRIB puns!

Session 5: Math Reading Groups

Anuj Sakarda and Jerry Tan

The Probabilistic Method

Mentor: YounHun Kim

The probabilistic method is a ubiquitous idea that has influenced number theory, graph theory, computational geometry and combinatorics. We will discuss the basic ideas behind the method, which is the core subject of Alon and Spencer's book. To serve as examples, we will discuss two applications which we found interesting: bounds on Ramsey numbers and Heibronn's triangle problem. Our presentation will include results that are known to be obtainable using the basic versions of the probabilistic method and its variants.

Yi (Alex) Liang

Representation Theory and Quantum Systems

Mentor: Sanjay Raman

Quantum physicists study representation theory extensively since it explains how a group acts on a quantum system. Unitary representations are of particular focus since they inherit the idea of symmetry, preserving certain aspects of the systems. In this presentation, by studying its unitary representation, we will offer some insights into the structure of the system that describes the spins of electrons — the two-state system.

Ilaria Seidel, Nathan Xiong, and William Yue

Dynkin Quivers and Their Representations

Mentor: Dr. Aleksandra Utiralova

Quivers are finite directed graphs that allow for loops and multiple edges between vertices. A representation of a quiver is an assignment of a finite-dimensional vector space to each vertex and a linear map to each directed edge. In this talk, we introduce Dynkin quivers, which are the only quivers with finitely many indecomposable representations. Finally, we state Gabriel's theorem, which classifies the indecomposable representations of Dynkin quivers.

SESSION 6: MATH READING GROUPS

Joshua Guo, Andrew Lee, and Karthik Seetharaman

Galois Theory and the Insolvability of the Quintic

Mentor: Chun Hong Lo

In this talk, we provide an exposition to Galois theory, an integral branch of classical algebra that connects field theory and group theory through the study of roots of polynomials. We begin by introducing the basic concepts of Galois theory such as fields, field extensions, splitting fields, and the Galois group. After this, we introduce the fundamental theorem of Galois theory, or Galois correspondence, which provides information about field extensions through their Galois group. Finally, we use this theorem to prove that polynomial equations of degree 5 or more are not solvable with just the four arithmetic operations and radical (i.e. there does not exist a "quintic formula"), which was one of the most famous unsolved problems in mathematics leading into the 19th century.

Kevin Zhao

Lie Matrices

Mentor: Sanjay Raman

Linear algebra and Lie groups are in close relation. Lie groups are used to solve linear algebra problems often, and vice versa. One topic that delves into both linear algebra and Lie theory is exponentials. With the Lie definition of exponentials, we can apply matrices to get very interesting results.

SESSION 7: PRIMES CIRCLE

Leisha Fortunat

A Simple Introduction to Graph Theory

Mentor: Rachana Madhukara

An introduction to graph theory is presented by giving definitions, numerous examples, and stating theorems. In particular, the presentation is split into three sections. First, the relevant definitions of graphs and their properties are explained along with examples. Then, we explore some very common classes of graphs and describe how they fit into the larger context of graph theory. Lastly, we discuss operations on graphs, such as the complement.

Daniela Yablon & Ayelet Yablon

Introduction to Cryptography

Mentor: Aparna Gupte

Cryptography is a cornerstone of modern communication, and is crucial to ensure security and privacy. In this talk, we describe two important encryption schemes — the RSA (Rivest–Shamir–Adleman) and Diffie Hellman encryption schemes. As quantum computers become more powerful, there is a very real possibility that these encryption systems will no longer remain secure, due to Shor's algorithm, developed by Peter Shor in 1994. We also describe how Shor's algorithm, using properties of quantum computers, can attack the RSA encryption scheme.

Zoe Siegelnickel & Palak Yadav

Algorithm Analysis

Mentor: John Shackleton

Algorithms are the foundation of technology today. From medicine to education and beyond, algorithms serve to solve complex problems. This talk explores several types of recursive algorithms and compares them using the conventional notation of time complexity. We analyze algorithms such as the Karatsuba algorithm and the Strassen algorithm, two kinds of algorithms that reduce the time it takes to multiply numbers.

Session 8: Computer Science

Rachel Chen

Uotchi: A Hardware Platform to Create and Exchange Non Fungible Objects

Mentor: Jules Drean

In the recent years, Non-Fungible Tokens have been all over the news. In particular, the possibility to exchange digital assets has garnered attention from the art industry, with auctions going as high as $69M to purchase a digital NFT artwork. There is a clear demand for a schema which enforces virtual ownership. However, the current implementation of NFTs presents several major flaws that greatly discredit the goal of the technology. Due to their shortcomings, independent artists and small businesses fall victim to digital theft and having their NFTs randomly disappearing from their owner's wallets.

To address these issues, we present Uotchis, a new type of secure hardware that enables the creation of non-fungible objects (NFOs) with a certificate of authenticity. We develop a local attestation mechanism, that can generate and update a proof of authenticity over our NFOs everytime it is edited, updated, or exchanged. We make sure our NFOs cannot be duplicated by introducing a heart-beat mechanism that ensures that the NFO only stays valid if it is actively stored on a Uotchi.

Abigail Thomas

The Implementation of Model Pruning to Optimize zk-SNARKs in Machine Learning

Mentor: Yu Xia

Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARK)s are used to convince a verifier that a server possesses certain information without revealing these private inputs. Thus, zk-SNARKs can be useful when outsourcing computations for cloud computing. The proofs returned by the server must be less computationally intensive than the given task, but the more complex the task, the more expensive the proof. We present a method that involves model pruning to decrease the complexity of the given task and thus the proof, as well, to allow clients to outsource more complex programs. When pruning the model, the number of constraints reduces from 363736 to 363719 when the model is pruned 50%, which decreases the time taken for training and the accuracy reduces from 0.9516 to 0.9505, an insignificant difference. Thus, the proposed method harnesses the benefits of producing accurate results using a lower number of constraints while remaining secure.

Tanisha Saxena

A Systematic Study on the Difference and Conversion Between Synchronous and Asynchronous Protocols

Mentor: Jun Wan

In this talk, we provide a fundamental analysis of the similarities and differences between synchronous and asynchronous distributed systems. Specifically, we define a special and normal adversary such that any protocol for a synchronous system that is resilient to the special adversary can be replicated by a protocol for an asynchronous system that is resilient to the normal adversary. Protocols for the synchronous model are less complex, as the guarantee that messages will be delivered within a bounded time makes it easy to determine the sequence of events in the system. But, this is unrealistic in the real world, as systems tend to be asynchronous where messages are not guaranteed to be delivered in a timely manner. Protocols for the asynchronous model, on the other hand, are more complex as there are many edge cases to account for. Our adversaries help to create intermediary models that allow us to replicate protocol outputs across both synchronous and asynchronous systems, allowing for simpler creation of protocols that remain functional under the asynchronous model.

Zifan (Carl) Guo

Understanding High-Level Properties of Low-Level Programs through Transformers

Mentor: William Moses

Transformer models have enabled breakthroughs in natural language processing, particularly using transfer learning, through which transformer models can be trained on a large corpus of unlabeled data. One can then perform fine-tuning on the model to fit a specific task. Unlike natural language with much tolerance of minor changes in word choices or ordering, programming languages' rigid structure means that their meaning can be completely redefined or invalid even if one token is altered. Furthermore, low-level languages, compared to high-level languages, are less expressive and more repetitive with more details of the computer microarchitecture, which makes understanding its semantics even harder for deep learning models.

Following successes in transformer models understanding of natural languages and high-level programming languages, this project explores how transformer models extrapolate high-level properties of low-level programs and transfer understanding of high-level programs to low-level programs through cross-lingual models. In particular, we show that transformer models can translate C to LLVM-IR with high accuracy by training on a parallel corpus of functions extracted from 1 million compilable, open-sourced C programs (AnghaBench) and its corresponding LLVM-IR. We discuss various changes in data selection, program representation, network architecture, and other modifications that influence the model's performance on low-level programs and can shed light on using transformer models to optimize compilers better.

Kevin Edward Zhao

Life after BERT: What Do Other Muppets Understand about Language?

Mentors: Prof. Anna Rumshisky and Vladislav Lialin, UMass Lowell

Existing pre-trained transformer analysis works usually focus only on one or two model families at a time, overlooking the variability of the architecture and pre-training objectives. In our work, we utilize the oLMpics benchmark and psycholinguistic probing datasets for a diverse set of 29 models including T5, BART, and ALBERT. Additionally, we adapt the oLMpics zero-shot setup for autoregressive models and evaluate GPT networks of different sizes. Our findings show that none of these models can resolve compositional questions in a zero-shot fashion, suggesting that this skill is not learnable using existing pre-training objectives. Furthermore, we find that global model decisions such as architecture, directionality, size of the dataset, and pre-training objective are not predictive of a model's linguistic capabilities.

Neil Chowdhury

A Mechanism of Formation for a Unique Compartment in the Silkworm Genome

Mentor: Sameer Abraham

Compartmentalization, one of the highest-level patterns in genome architecture, reflects how different classes of DNA organize spatially. Recently Hi-C contact maps produced from silkworm Bombyx mori larvae show that some chromatin domains exhibit significant intra-domain interactions, but do not significantly compartmentalize within euchromatin or heterochromatin. Furthermore, interactions between pairs of these domains are weak. The self-interacting domains thus form a novel compartment known as the X compartment. We propose that loop extrusion can create the unique contact patterns in X domains in a mechanism supported by experimental data and simulations of the molecular dynamics of chromatin.