Computations with a family of Kloosterman sums

Hideki Hill
Supervised by Dr. Cameron Franc

McMaster University
Department of Mathematics and Statistics
Undergraduate thesis presentations

April 7, 2025

Overview

History and introduction

Group theory background

Objectives and results

Research directions

Classical Kloosterman sums

- Introduced by Henrik Kloosterman, 1926
- Arising from the study of quadratic forms
- Define $K(a, b, n) : \mathbf{Z}^+ \to \mathbf{C}$ by

$$K(a, b, n) = \sum_{\substack{x=0 \\ gcd(x,n)=1}}^{n-1} e^{(ax+b\overline{x})\frac{2\pi i}{n}}$$

  where $\overline{x}$ is the multiplicative inverse of $x \mod n$.
- Frequently take n to be prime to be able to sum over every $0 \leq x \leq p-1$

Kloostermania

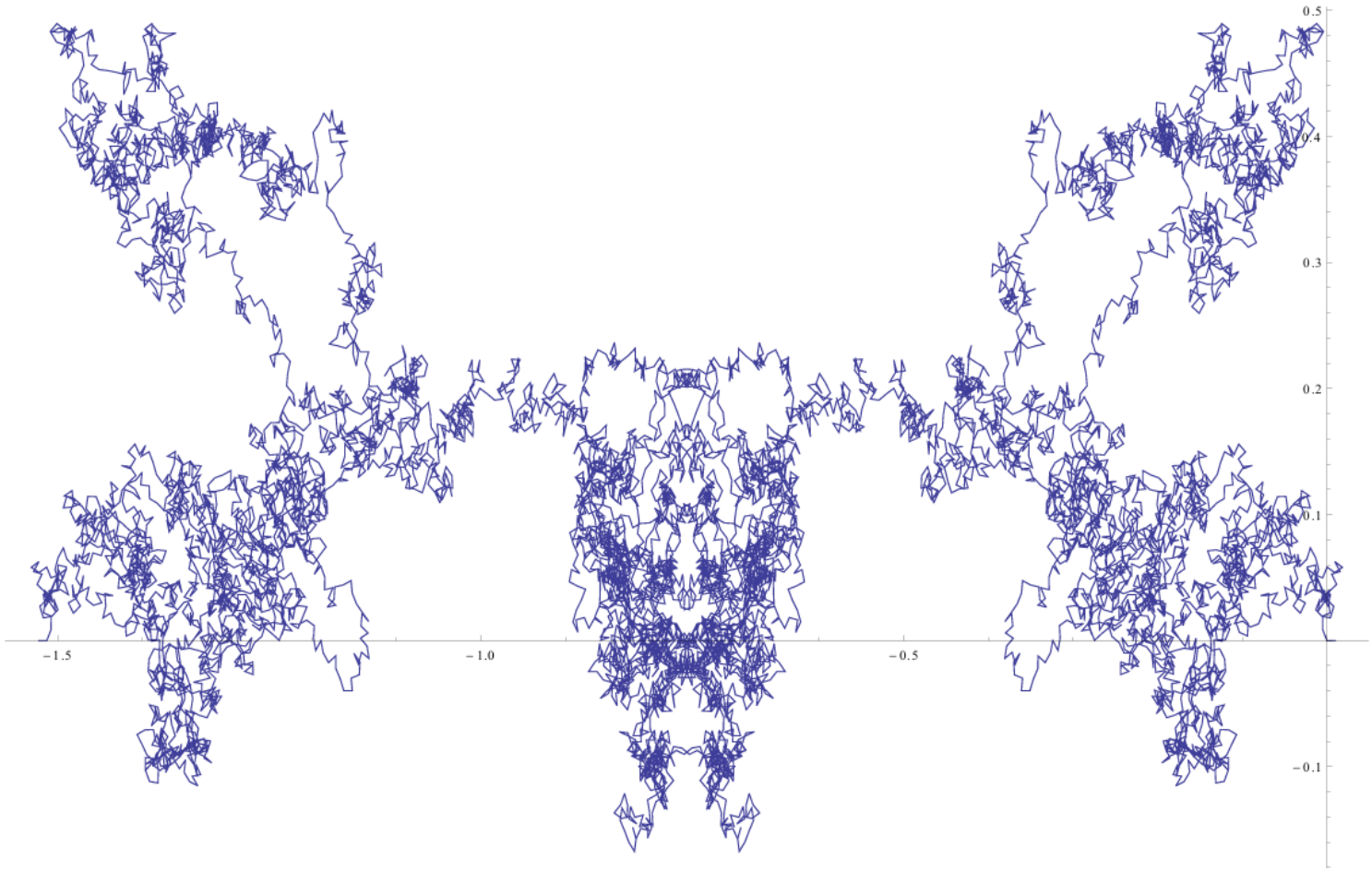

Figure: Normalized Kloosterman sum for $p = 10,007$ on the complex plane. Kowalski and Swain, 2016.

Appearances and applications

Kloosterman sums are useful in studying, for example, modular forms and elliptic curves when considering $\Gamma = SL_2(Z)$.

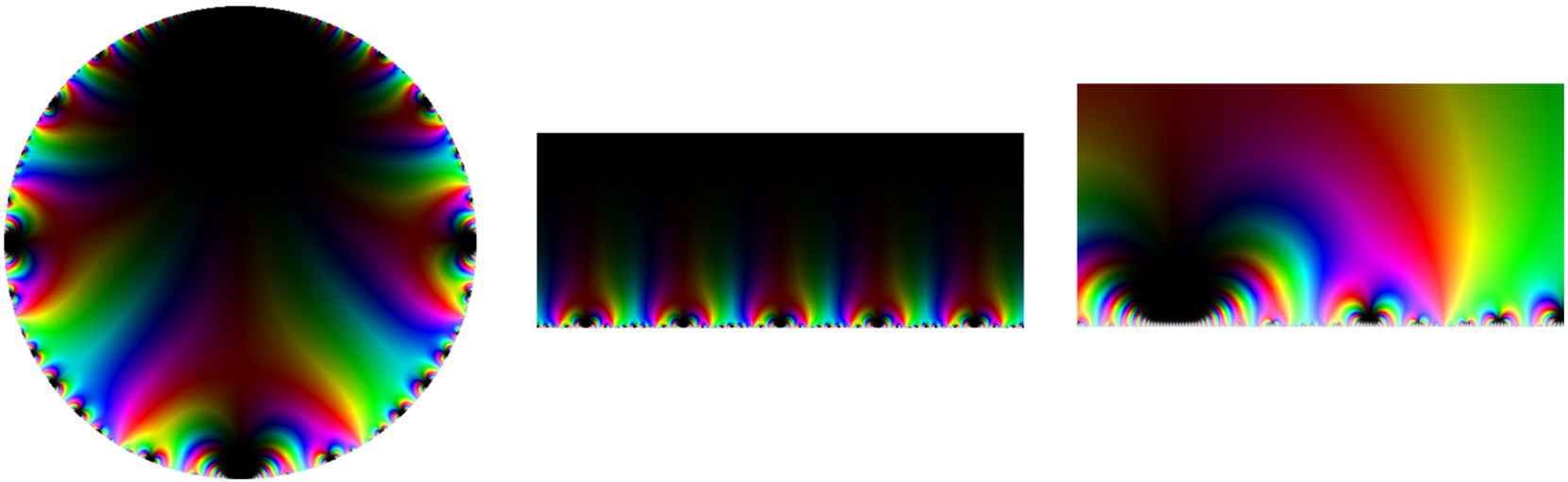

Figure: Visualizations of the modular form of weight 4 on $\Gamma(5) \subset SL_2(\mathbf{Z})$. Lowry-Duda, 2020.

Overview

Modular group

Definition

The **Modular Group** is the quotient of groups denoted by $\Gamma := SL_2(\mathbf{Z})/\{\pm 1\} = PSL_2(\mathbf{Z})$

- We will see shortly why this group is special
- It is known that $\Gamma = \langle S, T \rangle$ is generated by the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

- "Word problem": any element of Γ may be written as a product of powers of these generators
- Algorithmically solving the word problem will be useful when applying maps (representations) to arbitrary elements of the modular group

Example of word decomposition

Example

Let $g = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \in \Gamma$. We first apply S on the right of g resulting in

$$gS = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

Next, apply T on the right of gS resulting in

$$gST = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = S.$$

By right-multiplying both sides by $(ST)^{-1} = T^{-1}S^{-1}$, we see

$$g = ST^{-1}S^{-1}.$$

A modification of the Euclidean algorithm applies to any element of Γ in a similar way.

Representation theory basics

Definition

A **representation** of the modular group is a homomorphism between groups

$$\rho : \Gamma \to GL_d(\mathbf{C}).$$

We will take $d = 3$ for our purposes.

- We may apply representations on elements of Γ by exploiting the homomorphism properties on the word decomposition
- Surprisingly, representations of **finite image** exist. We may map each element of Γ to one of finitely many representations
- Further, some of these are **congruence**. We may classify where each element is mapped using congruence conditions
- The modular group is special since the intermediate representations of $SL_n(\mathbf{Z})$ exist *only* when $n = 2$

Illustration of representations

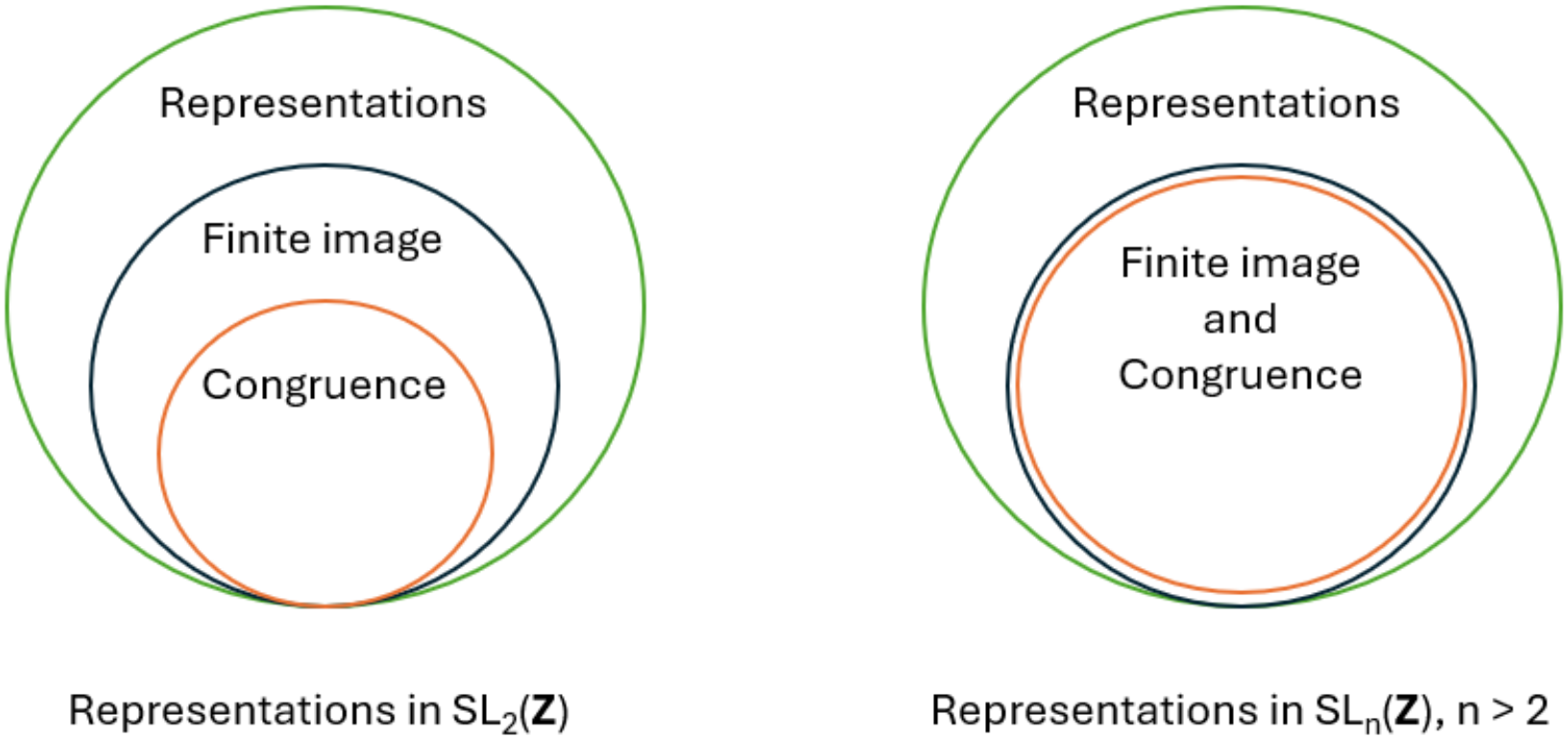

Figure: Difference in finite image representations of $SL_n(\mathbf{Z})$. Only when $n = 2$ do we see that the congruence representations are a proper subset of the finite image representations.

Special family of representations

For complex x, y we define:

$$\rho(T) = \begin{pmatrix} x & y^{-2}+y & y \\ 0 & y & y \\ 0 & 0 & x^{-1}y^{-1} \end{pmatrix}, \quad \rho(S) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Tuba and Wenzl showed that this family of representations of the modular group is unique up to twisting. Franc and Mason gave the following conditions:

1. $y = e^{2\pi im/n}, x = -y^{-2} \implies$ Finite image
2. $n \mid 24 \iff$ Congruence

The following results are based on a diagonalized version of this representation called $\phi_{x,y}$ obtained by conjugation on $\rho(T)$.

Matrix-valued Kloosterman sums and totient functions

Definition

Using the diagonalized representation $\phi_{x,y}$, define for integers $c \geq 1$ the corresponding family of **Kloosterman sums**:

$$K(x, y, c) = 4 \cdot \sum_{\substack{d=1 \\ \gcd(c,d)=1}}^{c} (\phi_{x,y} \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))^t \phi_{x^{-1},y^{-1}} \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$$

Definition

For $n \geq 1$, **Euler's totient function** at n, denoted $\varphi(n)$, is the number of integers relatively prime to n. Equivalently, the size of the multiplicative group of units modulo n:

$$\varphi(n) := |(\mathbf{Z}/n\mathbf{Z})^\times| = |1 \leq x \leq n : gcd(x, n) = 1|$$

Overview

Initial project objectives

Initial goals?

- Extend Dr. Franc's research on 2×2 representations to 3×3
- Formulate finitely many Kloosterman sums in congruence case
- Use results to compute residues of associated Dirichlet series
- Time permitting, explore a finite image non-congruence case

What did we do?

- Completed formulation of all Kloosterman sums in the intended congruence cases
- Computed various sums, proposed formulations, proved claims
- Computationally explored finite image non-congruence cases
- Made conjectures about formulations of non-congruence sums, a step toward understanding them

Example of congruence formulation

Proposition

Let $y \in \{e^{2\pi i \cdot 1/2}, e^{2\pi i \cdot 1/6}, e^{2\pi i \cdot 5/6}\}$ *and set* $x = -y^{-2}$. *Then for all* $c \geq 1$,

$$K(y,c) = \begin{cases} \begin{pmatrix} 5 & 3 & \frac{3}{2} \\ 3 & 9 & \frac{1}{2} \\ \frac{3}{2} & \frac{1}{2} & \frac{9}{4} \end{pmatrix} & c = 1 \\ \varphi(c) \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{pmatrix} & 2 \mid c \\ \varphi(c) \begin{pmatrix} 5 & 3 & 0 \\ 3 & 9 & 0 \\ 0 & 0 & \frac{9}{4} \end{pmatrix} & 2 \nmid c \end{cases}$$

Each of the congruence cases had similar results, but got successively more complicated.

Analysis of select sum entries

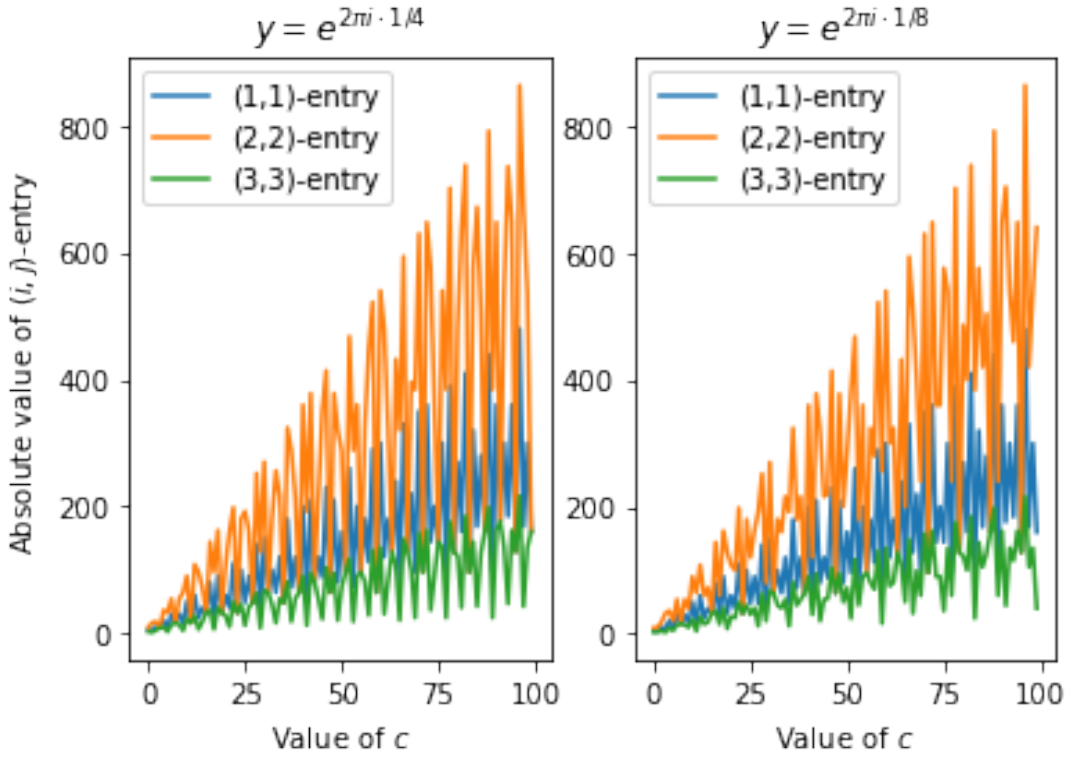

Figure: Absolute value of diagonal entries of $K(y, c)$ against c for select inputs of 4th and 8th roots of unity, depicting the linear growth of these entries.

Interesting non-congruence case

- We've claimed existence of non-congruence but finite image cases
- We consider the 9th root case, notice $9 \nmid 24$
- There are exactly 9 matrix terms appearing in the sum
- Whereas in the case of a 7th root, computations suggest at least 50 matrix terms appearing in the sum

Finitely many representations

For $\zeta = 1 + i\sqrt{3}$, begin by defining the following:

$$M = \frac{1}{4}\begin{pmatrix} 4 & 0 & 0 \\ 0 & 13 & \frac{3}{2}(\zeta - 1) \\ 0 & -\frac{3}{2}(\zeta - 1) & \frac{7}{4} \end{pmatrix},$$

$$A_1 = \frac{1}{4}\begin{pmatrix} 5 & -3 & -\frac{3}{2} \\ -3 & 9 & -\frac{1}{2} \\ -\frac{3}{2} & -\frac{1}{2} & \frac{9}{4} \end{pmatrix}, A_2 = \frac{1}{4}\begin{pmatrix} 5 & \frac{3}{2}\zeta & \frac{3}{4}\zeta \\ \frac{3}{2}\overline{\zeta} & 9 & \frac{1}{2} \\ \frac{3}{4}\overline{\zeta} & \frac{1}{2} & \frac{9}{4} \end{pmatrix},$$

$$B_1 = \frac{1}{4}\begin{pmatrix} 5 & -\frac{3}{2}\zeta & \frac{3}{4}\zeta \\ -\frac{3}{2}\overline{\zeta} & 9 & -\frac{1}{2} \\ \frac{3}{4}\overline{\zeta} & -\frac{1}{2} & \frac{9}{4} \end{pmatrix}, B_2 = \frac{1}{4}\begin{pmatrix} 5 & 3 & -\frac{3}{2} \\ 3 & 9 & -\frac{1}{2} \\ -\frac{3}{2} & -\frac{1}{2} & \frac{9}{4} \end{pmatrix}.$$

Table of values for the case $y = e^{2\pi i \cdot 1/9}$

Table: Number of times M_i, A_i, B_i appear in the sum $K(x, y, c)$

	$2 \mid c$			$2 \nmid c$			$2 \nmid c$		
c	I_3	M	M^t	A_1	A_2	A_2^t	B_1	B_2	B_1^t
1					1				
2			1						
3				1			1		
99				14	7	9	14	7	9
100	16	12	12						
101				15	18	17	15	18	17
256	42	36	50						
451				65	70	65	65	70	65
512	94	60	102						
625				71	89	90	71	89	90
1001				126	121	113	126	121	113
1024	150	174	188						
10,000	1460	1262	1278						

Primary result from noncongruence study

Conjecture

Let $y \in \{e^{2\pi i 1/9}, e^{2\pi i 4/9}, e^{2\pi i 7/9}\}$ *and set* $x = -y^{-2}$. *Then for* **odd** $c > 1$ *and integers* α, β, γ, *the Kloosterman sum is given by*

$$K(x, y, c) = \alpha(A_1 + B_1) + \beta(A_2 + B_2) + \gamma(A_2 + B_1)^t.$$

Similarly, for **even** $c > 1$, *the sum is given as a linear combination of* I_3, M, M^t.

This result is progress on understanding how sums are formed, since we are not able to understand them analytically through congruence. This narrows down the possibilities of formulation.

Overview

Analysis of associated Dirichlet series

One may associate to each Kloosterman sum a **Dirichlet series** that is analytic for $s > s_0$ where $K(x, y, c)$ grows of order s_0:

$$D(x, y, s) = \sum_{c \geq 1} \frac{K(x, y, c)}{c^s}.$$

Using my formulations in the congruence cases, residues may be computed at the pole $s = s_0$ (I believe $s_0 = 1$!). As stated, this was an initial goal, but we deviated to study the interesting case of non-congruence with great progress.

Further non-congruence

- Dr. Franc's research interests lie primarily in non-congruence finite image cases, my work advances this study
- The 9th root case we discussed today can be explored further, such as finding the three integers that determine the sum
- There are finite image sums other than this 9th root case to be explored

Key findings

- Formulated all Kloosterman sums in the congruence cases
- Laid groundwork to analyze associated Dirichlet series
- Made progress in study of Kloosterman sums in the finite image non-congruence case

Thank you

Thank you to Dr. Franc for supervising my project and to the Department of Mathematics and Statistics for this opportunity.