Intersection of conjugate solvable subgroups in $GL(n, q)$

Anton Baykalov  
*The University of Auckland*  
Supervisors: Eamonn O’Brien and Jianbei An  
a.baykalov@auckland.ac.nz

Assume that a finite group $G$ acts on a set $\Omega$. A point $\alpha \in \Omega$ is $G$-regular if $|\alpha^G| = |G|$, i.e. if the stabilizer of $\alpha$ is trivial. Define the action of the group $G$ on $\Omega^k$ by

$$(\alpha_1, \ldots, \alpha_k)g = (\alpha_1g, \ldots, \alpha_kg).$$

If $G$ acts faithfully and transitively on $\Omega$ then the minimal number $k$ such that the set $\Omega^k$ contains a $G$-regular point is the base size of $G$ and is denoted by $b(G)$. For a positive integer $m$ denote the number of $G$-regular orbits on $\Omega^m$ by $Reg(G, m)$ (this number is 0 if $m < b(G)$). If $H$ is a subgroup of $G$ and $G$ acts by the right multiplication on the set $\Omega$ of right cosets of $H$ then $G/H_G$ acts faithfully and transitively on $\Omega$. (Here $H_G = \cap_{g \in G} H^g.$) In this case, we denote $b(G/H_G)$ and $Reg(G/H_G, m)$ by $b_H(G)$ and $Reg_H(G, m)$ respectively.

In this work we consider Problem 17.41 b) from the "Kourovka notebook" [2]:

Let $H$ be a solvable subgroup of a finite group $G$ that has no nontrivial solvable normal subgroups. Do there always exist five conjugates of $H$ whose intersection is trivial?

The problem is reduced to the case when $G$ is almost simple in [3]. In particular it suffices to show that for every solvable subgroup $H < G$,

$$Reg_H(G, 5) \geq 5.$$

In [1] the inequality $Reg_H(G, 5) \geq 5$ is shown for almost simple groups with socle isomorphic to an alternating group $A_n$, $n \geq 5$.

The main statement of the present work is the following

**Theorem.** Let $G = GL(n, q)$, $n \geq 2$ and $(n, q)$ is not equal to $(2, 2)$ or $(2, 3)$. If $S$ is a maximal solvable subgroup of $G$ then $Reg_S(G, 5) \geq 5$, in particular $b_S(G) \leq 5$.

**References**


Title: How feedback mechanisms shape calcium oscillations in Hepatocytes

Speaker: Ielyaas Cloete

Supervisors: Prof James Sneyd and A/P Vivien Kirk

Variation of calcium concentration in hepatocytes (liver cells) is known to modulate diverse cellular functions, including bile secretion, glucose and energy metabolism and vesicular trafficking. A major question in the study of calcium signalling in hepatocytes is how these distinct cellular processes are controlled and organised via coordinated spatial and temporal calcium signals.

Downstream cellular responses are controlled via intracellular calcium oscillations but the underlying mechanisms which shape these oscillations have yet to be elucidated. We are interested in determining the effects of the calcium feedback on Phospholipase C (PLC) have on the whole-cell calcium signal. Recent experimental data suggests that hormone-induced calcium oscillations require positive calcium feedback on PLC to generate inositol trisphosphate oscillations, yielding cross-coupling between calcium and inositol trisphosphate.

This talk will discuss recent progress in construction and analysis of a model of calcium oscillations that incorporates the new experimental results about likely feedback mechanisms in hepatocytes.
CENTRALIZERS AND CONJUGACY CLASSES IN FINITE CLASSICAL GROUPS

GIOVANNI DE FRANCESCHI

SUPERVISORS: JIANBEI AN, EAMONN O’BRIEN

Classical groups are groups of matrices over finite fields. It is one of the most important class of finite groups, since many finite groups can be reconduced to classical groups. Moreover, they are one of the best known example of finite simple groups.

Classical groups include the general linear group GL(n, q) of all invertible n × n matrices over the field \( \mathbb{F}_q \) and the groups of isometries for non-degenerate alternating, quadratic or hermitian forms, denoted by Sp(n, q) (symplectic group), O(n, q) (orthogonal group) and U(n, q) (unitary group) respectively. Other classical groups are the special groups SL(n, q), SO(n, q) and SU(n, q), that are the subgroups of all matrices with determinant 1, and the Omega groups \( \Omega(n, q) \), the unique subgroup of SO(n, q) of index 2.

The aim of my PhD is to solve three problems about classical groups:

- Given a classical group \( G \), describe all the conjugacy classes of \( G \), and exhibit a representative for each of them.
- Given two elements \( x, y \) in \( G \), establish whether they are conjugate in \( G \) and, in such a case, provide an explicit \( z \in G \) such that \( z^{-1}xz = y \).
- Given \( x \in G \), describe the centralizer \( C_G(x) \) of \( x \) in \( G \), by describing its group structure and enlisting a small set of generators.

These three problems are closely related, often using the same type of arguments from finite group theory and linear algebra.

If \( G \) is a classical group over the field \( \mathbb{F}_q \), with \( q \) power of a prime \( p \), an element of \( G \) is semisimple (resp. unipotent) if its order is coprime with \( p \) (respectively is a power of \( p \)). The resolution of the semisimple and the unipotent case allows us with effort to resolve the general case.

During my PhD, I focused mainly on the semisimple case, starting from the work of Wall ([1]) and extending its results to the special and Omega groups. I then used the known results in the unipotent case (mainly from [2]) to sort out the general case.

In parallel to the theoretical research, I focused on the computational aspects, developing algorithms in Magma Language to compute explicitly the objects mentioned above.

In this talk I will show the main results of my research and briefly describe the technique used in the resolution of the semisimple case.

References


Investigating student narratives on gradient in a group antiderivative task

Rowan Herbert

Supervisors: Dr. Igor’ Kontorovich and A/Prof. Caroline Yoon

The transition from secondary school mathematics to the mathematics studied at tertiary level is known to be challenging. Amongst other obstacles to overcome, large class sizes translate into a more passive learning experience for students. As a way around this, group work is popular with some tertiary teachers as it has the potential benefit of allowing students to debate, discuss and learn without direct teacher involvement. My research investigates what kind of mathematics learning can occur in a group setting.

The data I am working with comes from video recordings of five pairs of students who worked on an antiderivative task. Their work occurred in the presence of an interviewer, who assisted the students with the task instructions but did not aid them mathematically. In my MProfStuds research I examine student interactions with each other and the interviewer from a communicational viewpoint. In particular, I am paying close attention to students’ generation of mathematical narratives and to how these are justified and endorsed when ‘expert advice’ is not readily available.

In this talk I will dissect one particular interaction where a pair of students tries to find the gradient at a particular point on a curve by drawing a tangent line. I will explore participant/interviewer dynamics as potential contributors to the emergence of a peculiar misconception.
Limits of Generalised Inverse Limits

Elizabeth Jagersma
Supervisor: Sina Greenwood

For each \( n \in \mathbb{N} \) let \( X_n \) be a topological space and let \( f_n : X_{n+1} \to X_n \) be a function. Then the sequence \( f = f_1, f_2, \ldots \) is called an inverse sequence, the sets \( X_1, X_2, \ldots \) are called factor spaces and the functions \( f_1, f_2, \ldots \) are called bonding functions. The set

\[
\lim_{\leftarrow} f = \left\{ (x_n) \in \prod_{n \in \mathbb{N}} X_n : \forall n \in \mathbb{N} \ x_n = f_n(x_{n+1}) \right\}
\]

is called the inverse limit of the inverse sequence \( f \), and has the topology inherited from the product space \( \prod_{n \in \mathbb{N}} X_n \).

We are concerned with inverse limits generated by a single bonding function (each \( f_n \) is a the same self-map). The graph of a function \( f : X \to X \) is the set

\[
\Gamma(f) = \{(x, y) \in X \times Y : y \in f(x)\}.
\]

Interestingly, if \( \langle f^n : X \to X | n \in \mathbb{N} \rangle \) is a sequence of surjective functions, and \( f : X \to X \) is a surjective function, then \( \Gamma(f^n) \) converges to \( \Gamma(f) \) with respect to the Hausdorff metric (which is equivalent to \( f^n \) converging to \( f \) pointwise) if and only if \( \lim_{\leftarrow} f^n \) converges to \( \lim_{\leftarrow} f \) with respect to the Hausdorff metric.

In 2004 a generalisation of inverse limits was introduced. Such generalised inverse limits have bonding functions which are allowed to be set valued. A natural question we can ask is: under what conditions will sequences of generalised inverse limits converge? Banič et al.\cite{Banič2010} found that if \( \langle f^n : X \to 2^X | n \in \mathbb{N} \rangle \) is a sequence of surjective set valued functions (\( 2^X \) is the collection of nonempty closed subsets of \( X \)), and \( f : X \to 2^X \) is a single valued surjective function (the image of each point is a singleton), then \( \lim_{\leftarrow} f^n \) will converge to \( \lim\!\!\!\!\!\!\!\!\!\downarrow f \) if and only if \( \Gamma(f^n) \) converges to \( \Gamma(f) \). However, relatively little is known about the convergence of generalised inverse limits when \( f \) is not single valued. In this talk, we will investigate sufficient conditions for these generalised inverse limits to converge, with a focus on finitely valued bonding functions.

References

Let $(X, d)$ be a metric space. The \textit{length} of a curve $c : [a, b] \rightarrow X$ is defined by

$$\sup_{a = t_0 \leq t_1 \leq \ldots \leq t_n = b} \sum d(c(t_i), c(t_{i+1})),$$

where the supremum is taken over all possible partitions of $[a, b]$. If the length of a curve is finite, we say that it is \textit{rectifiable}. A \textit{length space} is then a metric space whose distance between points is the infimum of lengths of curves between them. In this talk, we give various examples of these spaces and introduce some of their properties. The Hopf-Rinow Theorem is an important result on length spaces. We shall state this theorem and describe several corollaries.

\textbf{References}


Numerical study of airway smooth muscle and airway wall coupled dynamics.

Anand Rampadarath

Supervisor: Graham Donovan,
Co-supervisor: James Sneyd

Abstract

Asthma is fundamentally a disease of airway constriction. Due to a variety of experimental challenges, the dynamics of airways are poorly understood. Of specific interest is the narrowing of the airway due to forces produced by the airway smooth muscle (ASM) wrapped around each airway. The interaction between the muscle and the airway wall is crucial for the airway constriction which occurs during an asthma attack. While crossbridge theory is a well-studied representation of complex smooth muscle dynamics, and these dynamics can be coupled to the airway wall, this comes at significant computational cost -- even for isolated airways. Because many phenomena of interest in pulmonary physiology cannot be adequately understood by studying isolated airways, this presents a significant limitation. We present results associated with the development of an approximated method (distribution moment approximation) which provides orders of magnitude reduction in computational complexity whilst retaining rich ASM dynamics. This method is then used to model physiological processes such as airway contraction, bronchodilatory effect of a deep inspiration and preliminary results associated with heterogeneity of branched airways.
Analysis with slow-fast decomposition in a birdsong production model.

Pinki Rani
University of Auckland
Supervisor-Hinke Osinga

Slow-fast decomposition is a common method to identify different complex oscillating behaviour in systems with two different time scale. The birdsong production model introduced in [1] is a four-dimensional model with two fast variables and two slow variables. It models the dynamics of a membrane through airflow that generates sound waves for the bird. The slow variables for this model are the so-called sublabial pressure $p$ and a non-linear restitution force $k_1$. These two components are responsible for the oscillatory motion of the membrane that generates different spectral content producing sound of different fundamental frequencies.

The analysis of the dynamics presented by this model starts with the classical analysis of the fast subsystem that is obtained by treating $p$ and $k_1$ as parameters [2]. We use bifurcation theory and compute the bifurcation diagram in the $(p_r,k_1)$-plane, where $p_r$ is a scaled version of $p$. To this end, we calculate all fixed points, their stability, and observed types of local and global bifurcations like saddle-node, cusp, Hopf and homoclinic bifurcations. The Hopf bifurcation is responsible for the periodic motion and creates periodic orbits of different periods. We focus on a particular region of the $(p_r,k_1)$-plane and compute curves along which the periodic orbits have a specific, fixed period. These curves of fixed period combined with details on the different amplitudes of the periodic orbits, provide information about which parameter values generate the various phases of spectral content in a bird’s song.

References:


Mostafa Raziebrahimsaraei

Supervisors:
Dr. Jeroen Schillewaert
D. Prof. Marston Conder

Abstract

Buildings are a class of geometries introduced by J. Tits [Ti1, Ti2] to study (exceptional) algebraic groups. They have found applications in several areas of mathematics including number theory and differential geometry.

The Freudenthal-Tits magic square [Fr, Ti3] is given by the following table:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>K</th>
<th>L</th>
<th>H</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>K</td>
<td>A1</td>
<td>A2</td>
<td>C3</td>
<td>F4</td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>A2</td>
<td>A2 × A2</td>
<td>A5</td>
<td>E6</td>
<td></td>
</tr>
<tr>
<td>H</td>
<td>C3</td>
<td>A5</td>
<td>D6</td>
<td>E7</td>
<td></td>
</tr>
<tr>
<td>O</td>
<td>F4</td>
<td>E6</td>
<td>E7</td>
<td>E8</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: The Magic Square

The square gives a uniform construction of the exceptional algebraic groups starting from two composition algebras. In this talk, we will focus on the projective varieties associated to the $C_3$ entry.

References

The transmission problem in forward and inverse scattering

Scarlett Shi
Supervisor: Jari Kaipio

Abstract

Scattering theory is a framework for studying the processes in which waves are scattered from impenetrable or penetrable obstacles/scatterers. The inverse scattering problem is to determine the characteristics of a scatterer based on measurement data of the (sound) field. In this talk, we consider two models for the forward transmission problem, and the final aim is to recover the distribution of wavenumber function $k(x)$ of a bounded scatterer from the observation data.

To begin with, an analytical and numerical investigation of forward scattering using finite element method (FEM) is discussed. Then we consider an equivalent integral equation of the forward scattering problem: the Lippmann-Schwinger equation. For weak scatterer, its solution can be represented using Born series. We also study the conditions of $k(x)$ that would guarantee the convergence of Born series for our example. Finally, we consider the corresponding ill-posed inverse transmission problem, which is to estimate the wavenumber function $k(x)$ based on the observation data. In the inverse problem, we use a linear approximation for the nonlinear forward operator, which is called the Born approximation. Then we use Tikhonov regularization to obtain a well-posed approximation of this inverse problem.
**Student:** Elias Siguenza

**Supervisor:** James Sneyd

**Title:** Stick your tongue out and look in the mirror, is it dry?

**Abstract:**

Saliva plays an important role in our daily lives. It is mostly comprised of water but it also contains important substances that our body needs in order to digest food and keep a good oral hygiene. Certain diseases, medicines, and cancer treatments affect how much saliva an individual makes. This causes the gums, tongue, and other oral tissues to become swollen and uncomfortable, and in extreme cases, rotting of the mouth. To treat and/or cure these ailments, we must understand how saliva is produced.

The currently accepted saliva secretion model uses the chloride ion as the rate limiting step for water transport. In salivary gland acinar cells, membrane mechanisms introduce and elevate intracellular chloride well above its electrochemical gradient. Once its concentration is high, calcium ions are used as signalling messengers to promote chloride efflux. The net transcellular passage of chloride ions generates an osmotic gradient which water follows (by the principle of osmosis).

We use a 3-dimensional cell dynamic model to investigate how the spatio-temporal properties of calcium signalling affect the way these cells produce saliva. Our results suggest that the way calcium signals travel across the diverse regions of the cell encode information critical for saliva secretion.
A characterisation of distinguished curves

Daniel Snell
Supervisor: A. Rod Gover

This is joint work with Rod Gover and Armann Taghavi-Chabert.

On a Riemannian manifold $(M, g)$, one has a unique connection which preserves the metric: the Levi-Civita connection [1]. The geodesics of such a connection are classically well-studied and are known to be linked to conserved quantities.

Projective and conformal geometry are generalisations of Riemannian geometry, and come with their own notions of geodesics [2]. In both cases, one studies a manifold equipped with an equivalence class of connections (respectively metrics), and thus there is no longer a unique connection on the tangent bundle. Tractor calculus [3] gives a vector bundle of slightly higher rank which possesses a unique connection respecting the more general geometry. This connection then plays much the same role as the Levi-Civita connection does in Riemannian geometry.

Our current work provides a parametrisation-independent characterisation of these curves for the respective geometries, stated entirely in terms of tractor calculus. Conserved quantities are also nicely incorporated in this framework.

In this talk, I will introduce tractor calculus machinery for projective and conformal geometries, present our characterisation of the respective geodesics and discuss some examples of conserved quantities via elements of BGG theory [4].

References


Elliptic Operators with Boundary Conditions

Chris Wong
Supervisor: Tom ter Elst

Consider the elliptic operator

\[ A = - \sum_{k,l=1}^{d} \partial_k c_{kl} \partial_l - \sum_{k=1}^{d} \partial_k b_k + \sum_{k=1}^{d} a_k \partial_k + c_0 \]

on a bounded connected open set \( \Omega \subset \mathbb{R}^d \) with Lipschitz boundary conditions, where \( c_{kl} \in L_\infty(\Omega, \mathbb{R}) \) and \( a_k, b_k, c_0 \in L_\infty(\Omega, \mathbb{C}) \) for all \( k, l = 1, 2, ..., d \), subject to Robin boundary conditions \( \partial_\nu u + \beta \text{Tr} u = 0 \). It is possible to show that the semigroup generated by \( -A \) admits a kernel with Gaussian estimates and Hölder Gaussian estimates for a certain class of \( \beta \).

In this talk, we will show that such estimates can be extended to all complex measurable \( \beta \). We will also explain how that can be applied to obtain other bounds such as lower bounds for the kernel.
Abstract

Composition algebras arise naturally in mathematics and physics. The most important example is $\mathbb{C}$, which is a 2-dimensional vector space over the $\mathbb{R}$. Other examples include quaternion algebras which are 4-dimensional and octonion algebras which are 8-dimensional. We will give a complete proof of Hurwitz’s Theorem which states that the only possible dimensions are 1, 2, 4, and 8. We will also investigate the algebraic structures of composition algebras and their classification.

In Chapter 1 we introduce field algebras, quadratic forms, (non)degeneracy, isotropy, and isometry, we will also state/derive some important results including Witt’s Extension Theorem, which becomes useful in Chapter 4. In Chapter 2 we introduce composition algebras and explore some interesting properties such as Moufang identities and alternative laws. In Chapter 3, we investigate properties such as associativity and commutativity, leading to the conclusion that composition algebras cannot have dimensions greater than 8. In Chapter 4, we study the algebraic structures of composition algebras over different field characteristics; we will also classify composition algebras over finite fields and algebraically closed fields, and show that the maximum dimension of a finite division composition algebra is 2.
Stability analysis of swirling flow in a finite-length pipe

Weimin Yuan supervised by Shixiao Wang

Abstract

The three-dimensional, viscous flow instability modes that appear on a top-lid rotation flow in a finite-length, straight, circular pipe are analysed. This study is a direct extension of the Wang & Rusak [1] [2] [3] analysis of axisymmetric instabilities on inviscid swirling flows in a pipe. The linear stability equations are the same as those derived by Kelvin [4]. However, we study a general mode of perturbation that satisfies no-slip wall conditions of a flow in a finite-length pipe with a rotating top-lid. This mode is different from the classical normal mode of perturbations. The eigenvalue problem for the growth rate and the shape of the perturbations for any azimuthal wavenumber m consists of a linear system of partial differential equations in terms of the axial and radial coordinates (x; r). The stability problem is solved numerically for all azimuthal wavenumbers m. Velocity trajectory that shows linear stage and the nonlinear stage of the axial velocity evolution reveals the existence of attractor in the global dynamics of perturbations on the top-lid rotation flow. We use the Reynolds-Orr equation to analyse the various production terms of the perturbation’s kinetic energy, and establish that the elimination of the flow axial homogeneity as the underlying physical mechanism that leads to flow exchange of stability and to the appearance spiral instabilities. The viscous effects in the bulk have only a passive influence on the modes’ shapes and growth rates.

References

Cryptographic Trilinear Maps

Lukas Zobernig
Supervisor: Steven D. Galbraith

The Weil pairing was introduced by André Weil for Jacobians of curves in 1940 [1]. In modern definition for elliptic curves it is a bilinear map \( e_l : E[l] \times E[l] \rightarrow \mu_l \) where \( E[l] \) is the \( l \)-torsion subgroup of some suitable elliptic curve \( E \) and \( \mu_l \) the group of \( l \)-th roots of unity, such that \( \forall a, b \in \mathbb{Z} \)

\[
e_l(aP, bQ) = e_l(P, Q)^{ab}.
\]

It took many years of neglect from cryptographers to finally recognise it as a useful tool. A major breakthrough was made by using the Weil pairing for tripartite Diffie–Hellman key exchange which subsequently resulted in the cryptographic world erupting with numerous novel constructions and coining the term pairing based cryptography [2].

Nowadays cryptographers have developed a new fad called program obfuscation. One possible way to achieve this is by exploiting the duality of programs and circuits which in turn can be rewritten into matrix branching programs [3]. It was hoped that these matrix branching programs could be cryptographically encoded using pairings. The best constructions at the moment require at least a cryptographic trilinear map, i.e. a map \( f : G \times G \times G \rightarrow G_T \) such that \( \forall a, b, c \in \mathbb{Z} \)

\[
f(aP, bQ, cR) = f(P, Q, R)^{abc}
\]

and such that the discrete logarithm problem (DLP) is hard in the groups \( G \) and \( G_T \). We say that the DLP is hard in \( G \) if given \( g \in G \) and \( g^a \in G \) it is hard to find \( a \).

In this talk we will describe a recent candidate for a cryptographic trilinear map as in equation (1) on principally polarised abelian surfaces and a concrete construction using supersingular high genus curves as well as some of its constraints and shortcomings [4].

References


