Modelling pulse propagation along an optical fibre with higher-order dispersion – do such solitons exist?

Ravindra Bandara
Supervisors : Bernd Krauskopf and Neil Broderick

The generalized non-linear Schrödinger equation (GNLSE) is a nonlinear partial differential equation (PDE) that describes many diverse physical phenomena, e.g., the propagation of light in optical waveguides, the dynamics of Bose-Einstein condensates and small-amplitude gravity waves in the ocean. In general, analytical solutions for the GNLSE are hard to find, especially, when considering higher-order dispersion. We are concerned with pulse propagation in photonic crystal fibre where the dispersion is dominated by fourth-order terms. Some solutions have been found numerically recently [1], and shown to propagate stably over multiple dispersion lengths of the fibre; these solutions feature oscillating tails. We consider a stationary wave solution ansatz, where the optical pulse does not undergo a change in shape while propagating. This allow us to transform the PDE into a fourth-order nonlinear ordinary differential equation (ODE). In particular, soliton solutions of the PDE corresponds to homoclinic orbits of the ODE. It is known that there may be infinitely many symmetric homoclinic orbits in fourth-order reversible ODEs depending on the non-linearities [2]. We employ numerical continuation techniques to show that the GNLSE for the photonic crystal fibre has infinitely many homoclinic orbits, hence there are infinitely many solitons solutions of the fourth-order NLSE.

References:

1. Blanco-Redondo, A., De Sterke, C. M., Sipe, J. E., Krauss, T. F., Eggleton, B. J., & Husko, C. (2016). Pure-quartic solitons. *Nature communications*, *7*, 10427

2. Champneys, A. R. (1998). Homoclinic orbits in reversible systems and their applications in mechanics, fluids and optics. *Physica D: Nonlinear Phenomena*, *112*(1-2), 158-186.

Intersection of conjugate solvable subgroups in linear and unitary finite groups

Anton Baykalov

Supervisors: Eamonn O'Brien and Jianbei An

a.baykalov@auckland.ac.nz

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

Problem. *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 existence of such conjugates of H is equivalent to the statement that the **base size** of G with respect to its action on right cosets of H by right multiplication is at most 5.

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

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

If G acts faithfully and transitively on Ω then the minimal number k such that the set Ω^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 Ω^m by $Reg(G, m)$ (this number is 0 if $m < b(G)$). If H is a subgroup of G and G acts by right multiplication on the set Ω of right cosets of H then G/H_G acts faithfully and transitively on Ω. (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.

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, $n \geq 5$. In particular $b_H(G) \leq 5$.

In this talk we summarise the outcome for $GL(n, q)$ and discuss the current progress on the case $GU(n, q)$.

References

[1] A.A. Baikalov, Intersection of conjugate solvable subgroups in symmetric groups, *Algebra and Logic*, Vol. **56**, No. 2, (2017) 87–97

[2] Victor D. Mazurov and Evgeny I. Khukhro, *Unsolved problems in group theory. The Kourovka notebook*, No **18**. URL: http://arxiv.org/abs/1401.0300

[3] E. P. Vdovin, On the base size of a transitive group with solvable point stabilizer, *J. Algebra Appl.* 11 (2012), no. **1**, 14 pp.

Representations of quivers and dense orbits

Sean Carroll
in collaboration with Dr. Asilata Bapat and Dr. Anand Deopurkar,
Masters Supervisor: Dr. Jeroen Schillwaert

May 16, 2019

Abstract

It is well known that $\mathbb{P}\mathrm{GL}_2(\mathbb{C})$ acts 3-transitively on $\mathbb{P}^1$. However, $\mathbb{P}\mathrm{GL}_3(\mathbb{C})$ does not act transitively on the space of all configurations (l_1, l_2, p_1, p_2) in $\mathbb{P}^2$ where l_1, l_2 are distinct lines and p_1, p_2 are distinct points not contained in l_1 or l_2. Such problems are special cases of the *n subspace problem* in algebraic geometry, which asks when n subspaces have a dense orbit in $\mathbb{P}^m$ under the diagonal action of $\mathbb{P}\mathrm{GL}_m(\mathbb{C})$.

In [1] Coskun, Hadian and Zakharov proved the existence of dense orbits only in certain cases; namely, when the number of subspaces is less than 5 and when the dimension of the subspaces is bounded.

To extend their work to more general configurations we use *quivers* [2], which allow us to study the problem with representation theory. We give necessary and sufficient conditions for when a dense orbit occurs, as well as an algorithm for testing the existence of a dense orbit.

This work was undertaken in the summer of 2018/19 at Australia National University in Canberra, supported by an ANU summer research grant.

References

[1] Izzet Coskun, Majid Hadian, and Dmitry Zakharov. Dense pgl-orbits in products of grassmannians, 2014.

[2] Michel Brion. Representations of quivers. Notes de l'école d'été "Geometric Methods in Representation Theory", 2008.

Nonstationary inverse problems in practice

Pascal Eun Sig Cheon
Supervisor: Dr. Jari Kaipio

The main goal of inverse problems is to estimate the unknown quantity. These problems are come across in many scientific areas, including geophysical near-surface imaging, medicine, weather forecasting, and physical parameter estimation.

Inverse problems can be largely categorised into stationary inverse problems and nonstationary inverse problems. As the name suggests, stationary inverse problems involve a time-invariant unknown like in X-ray imaging. Nonstationary inverse problems involve a time-variant unknown like in weather forecasting.

Computational complexity concerns may be raised especially in nonstationary inverse problems because the estimates need to be updated in real time. My research focus involves developing estimation techniques for nonstationary inverse problems to make the computations more efficient.

In this talk, we show an approach to “solving" a nonstationary inverse problem from scratch with a special focus on improving the computational efficiency. As a numerical demonstration, we use an industrial problem, known as the pipeline monitoring.

CR geometry and its distinguished curves

Daniel Snell

Supervisor: A. Rod Gover

A CR manifold consists of a smooth manifold M of real dimension $2n+1$, together with a rank n distinguished complex subbundle H of the tangent bundle.

CR manifolds are a class of classically studied manifold, motivated by the problem of understanding the geometry of a real hypersurface in $\mathbb{C}^n$.

A useful and important result in the study of CR manifolds is due to Fefferman: for any CR manifold M of real dimension $2n+1$, one can construct a manifold $\tilde{M}$ of real dimension $2n+2$ which is the total space of a circle bundle over M. The manifold $\tilde{M}$ is called the *Fefferman space* [1].

In addition, the CR structure on M induces a conformal structure on the Fefferman space in such a way that conformal data on $\tilde{M}$ encodes CR data from M. This suggests an alternative approach to studying CR geometry: one instead studies the simpler conformal geometry of the Fefferman space.

More recently, CR manifolds have been studied under the framework of *tractor calculus*, which can also be applied to the study of projective or conformal manifolds. The correspondence described is also nicely understood via tractor methods [2]. However, unlike the aforementioned examples which are both *1-graded* geometries, CR manifolds are an example of a *2-graded* geometry, and thus admit a much richer theory of distinguished curves.

In this talk, we will discuss the Fefferman correspondence from the tractor perspective, as well as describing some of the classes of CR-distinguished curves, and how this fits into our existing theory of distinguished curves in projective and conformal geometry [3].

References

[1] C. L. Fefferman, "Monge-Ampère Equations, the Bergman Kernel, and Geometry of Pseudoconvex Domains," *Annals of Mathematics*, vol. 103, no. 3, pp. 395–416, 1976.

[2] A. Čap and A. R. Gover, "CR—tractors and the Fefferman space," *Indiana University Mathematics Journal*, vol. 57, no. 5, pp. 2519–2570, 2008.

[3] A. R. Gover, D. Snell, and A. Taghavi-Chabert, "Distinguished curves and integrability in Riemannian, conformal, and projective geometry," *arXiv preprint arXiv:1806.09830*, 2018.

Generalised Stone Dualities

David Farrell
Supervisor: Pedram Hekmati

In 1938, Marshall H. Stone, motivated by his work in functional analysis, proved his *representation theorem for Boolean algebras*, which establishes a correspondence [1] between a certain class of posets, called *Boolean algebras*, and a certain class of topological spaces, called *Stone spaces*. This correspondence, after the inception of category theory in the 40s, was recognised to be a *duality of categories*.

More recently, it has been found that there exists a similar correspondence between the category of those topological spaces satisfying a weak separation condition called *sobriety* and the category of posets, called *spatial locales*, which satisfy a set of axioms analogous to those for a topology [2]. A slight weakening of the conditions on spatial locales yields *locales*, which can be shown to satisfy many nice properties. For example, the analogue for Tychonoff's theorem for locales has a constructive proof. The theory of locales is considered to be a model of *point-free topology*, since the spaces considered do not have a primitive notion of *point*.

The duality between sober topological spaces and spatial locales is one of a number of theorems given the name *Stone duality*. In this talk I give a further generalisation of the methods of Stone duality which provides a duality theorem for any category of posets which satisfies a handful of weak conditions. Special cases include Stone's representation theorem for Boolean algebras, the duality between sober spaces and spatial locales, and a correspondence between a category of Boolean algebras and a subcategory of measurable spaces. I will sketch a proof for this new formulation of Stone duality, prove an original result for the duality for measurable spaces and give some results of Loomis [3] in the new context.

References

[1] Peter T. Johnstone, *Stone Spaces*, Cambridge University Press, 1982.

[2] Jorge Picado and Aleš Pultr, *Frames and Locales: Topology without points*, Springer Basel AG 2012.

[3] L. H. Loomis, *On the representation of σ-complete Boolean algebras*, Bull. Amer. Math. Soc. 53 (1947), pages 757-760.

Asymptotic Curvature of Constant Mean Curvature Hypersurfaces in Minkowski Space

Shintaro Fushida-Hardy
Supervised by Professor Rod Gover

Abstract

The asymptotic curvatures of certain space-like hypersurfaces in Minkowski space are investigated using conformal tractor calculus [BEG94]. Given a conformally compact manifold M and a choice of scale, it is shown that the corresponding scale tractor I determines the asymptotic curvature. In particular, M is asymptotically hyperbolic if $|I|^2$ tends to 1 at conformal infinity. Understanding the asymptotic curvatures of hypersurfaces then becomes the question of understanding how hypersurface scale tractors relate to ambient scale tractors.

Extending results from [GWss] concerning hypersurface tractor calculus in Riemannian manifolds to Lorentzian signature ambient spaces, formula (6.6) in [FH18] relating intrinsic hypersurface scale tractors and ambient scale tractors is obtained. It follows that non-vanishing constant mean curvature space-like hypersurfaces in Minkowski space are asymptotically hyperbolic. Finally, the result is generalised to such hypersurfaces in arbitrary asymptotically flat spacetimes.

References

[BEG94] T. N. Bailey, M. G. Eastwood, and A. Rod Gover. Thomas's structure bundle for conformal, projective and related structures. *The Rocky Mountain Journal of Mathematics*, 24(4):1191–1217, 1994.

[FH18] Shintaro Fushida-Hardy. *Asymptotic Curvature of Hypersurfaces in Minkowski Space*. BSc (Hons) dissertation. University of Auckland, 2018.

[GWss] A. Rod Gover and Andrew Waldron. A Calculus for Conformal Hypersurfaces and new higher Willmore energy functionals. *Advances in Geometry*, in press.

Modelling task switching with noisy heteroclinic networks

Gray Manicom, under the supervision of Claire Postlethwaite and Vivien Kirk

There are two types of people in this world: those who think they are good at multitasking, and those who are correct. People who think that they are good at multitasking are actually worse at it than those who do not.[1] This is related to the implicit time cost for task switching, called the switch cost. Psychologists are interested in this phenomena and how it varies from person to person. My research project involves trying to understanding the phenomena of task switching by modelling it using a dynamical object called a noisy heteroclinic network.

Heteroclinic networks are special solutions of dynamical systems in which trajectories cycle between various states, such as saddle type equilibrium solutions or periodic orbits. These heteroclinic networks are structurally stable in cases where the underlying system of ODEs has symmetries, and thus there existing invariant subspaces which contain the connecting heteroclinic orbits. The deterministic behaviour of these systems is, in some cases, well understood. However, with the addition of noise to the system its behaviour can change significantly. The noisy system may exhibit dynamics such as switching between the network's subcycles, a change in the residence times of trajectories near the aforementioned states, and lift off. Lift off occurs when a noisy trajectory no longer lies within the invariant plane containing the heteroclinic connection, causing the system to manifest non-Markovian dynamics.[2]

It is the presence of memory in these systems that makes them suitable tools to model task-switching, since a person's performance at a task depends on whether they have switched from another task or not.

References

[1] Sanbonmatsu, David M., et al. "Who multi-tasks and why? Multi-tasking ability, perceived multi-tasking ability, impulsivity, and sensation seeking." *PloS one* 8.1 (2013): e54402

[2] Armbruster, D, Emily S, and Vivien K. "Noisy heteroclinic networks." *Chaos: An Interdisciplinary Journal of Nonlinear Science* 13.1 (2003): 71-79.

Short presentations of alternating and symmetric groups

Peter Huxford

Supervisor: Professor Eamonn O'Brien

The *bit-length* of a presentation is the total number of symbols required to write it down, where each generator is a single symbol, each relator is a string of symbols, and exponents are stored in binary.

Presentations with short bit-length have applications in computational group theory. A major project is to compute a composition series of a matrix group over a finite field. In [Lee01] Leedham-Green discusses a randomised algorithm to solve this problem. To check correctness of the resulting composition series, a presentation of the input group is constructed using presentations of the composition factors. If the relations are satisfied in the input group, then the constructed composition series is correct. In order for this verification step to be efficient, the presentations of the composition factors, which are finite simple groups, must have short bit-length.

In [GKKL11] Guralnick, Kantor, Kassabov and Lubotzky define presentations of A_n and S_n for $n \geq 5$ with 3 generators, 7 relations, and bit-length $O(\log n)$. This is the smallest possible bit-length, since $\log n$ bits are required to describe n in the input. However, the proposed generators do not satisfy the relations. The correctness of these presentations is crucial for the short presentations given in the paper of other finite simple groups.

In this talk we discuss the relevant arguments given in [GKKL11], identify where the errors occur, and show how they can be fixed in order to recover this result.

References

[GKKL11] R. M. Guralnick et al. "Presentations of finite simple groups: a computational approach". *J. Eur. Math. Soc. (JEMS)* 13.2 (2011), pp. 391–458.

[Lee01] Charles R. Leedham-Green. "The computational matrix group project". *Groups and computation, III (Columbus, OH, 1999)*. Vol. 8. Ohio State Univ. Math. Res. Inst. Publ. de Gruyter, Berlin, 2001, pp. 229–247.

Evolving robots that have heteroclinic brains

Valerie Jeong

Supervisors: Claire Postlethwaite and Matthew Egbert

Artificial neural networks play a key role in a field called Evolutionary Robotics. These networks are the controllers of robots, and they are evolved so that such robots can successfully carry out a task. The controllers are often modelled using continuous-time recurrent networks (CTRNNs) [1]. Recently, we have investigated another architecure in the form of heteroclinic networks, motivated by the use of heteroclinic networks to describe the dynamics of neuronal activity in the brain [4]. Our work shows that heteroclinic networks work well as controllers in a Evolutionary Robotics task [2]. However, it is not well understood why heteroclinic networks work as a controller. This raises the need for further analysis of the dynamics of heteroclinic networks, especially with inputs and/or noise.

In this talk, I will describe how we use heteroclinic networks as a controller in Evolutionary Robotics, and discuss what happens when we perturb a simple heteroclinic network called the Guckenheimer-Holmes cycle [3].

References

[1] R. D. Beer, "On the dynamics of small continuous-time recurrent neural networks," *Adaptive Behavior*, vol. 3, no. 4, pp. 469–509, 1995.

[2] M. D. Egbert, V. Jeong, and C. M. Postlethwaite, "Where computation and dynamics meet: Heteroclinic network-based controllers in evolutionary robotics," *IEEE Transactions on Neural Networks and Learning Systems*, To be published.

[3] J. Guckenheimer and P. Holmes, "Structurally stable heteroclinic cycles," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 103, no. 1, 189–192, 1988.

[4] M. Rabinovich, P. Varona, I. Tristan, and V. Afraimovich, "Chunking dynamics: Heteroclinics in mind," *Frontiers in Computational Neuroscience*, vol. 8, p. 22, 2014.

Investigations of an unpublished John von Neumann manuscript on boostered detonations

Molly Riley Knoedler
Supervised by Chad Higdon-Topaz,
Professor of Mathematics at Williams College, MA, USA
Commitee Member: Shixiao Wang

May 16, 2019

Abstract

The scientific community made major leaps in shock wave and detonation theory at the end of the 19th and into the 20th century. Among the key mathematicians this field was John von Neumann, whose accomplishments include contributing to the development of the 1-dimensional model of detonation, ZND theory, in addition to other innovative work concerning oblique reflections of shock waves. In total, von Neumann's (declassified) body of work concerning shocks consists of 11 papers published between 1941 and 1955 [2].

This talk concerns an unpublished manuscript handwritten by John von Neumann at an unknown date. The goal of the manuscript is to derive an analytical, generalizable ratio of booster material to main charge in any boostered explosive in order to ensure successful detonation. We will discuss the foundational elements of shock theory such as the Rankine-Hugoniot equations and the Chapman-Jouget Hypothesis [1], the assumptions of the model proposed by von Neumann, and how the model compares to those in his published works. Although we conclude that the model is of minimal practical usefulness, as some of von Neumann's assumptions violate the rules of detonation we know today, the document is a valuable historical record of the techniques used in the development of detonation theory.

References

[1] Dremin, A. N. *Toward detonation theory.* Springer Science & Business Media, 2012.

[2] Von Neumann, J. Collect works, vol. 5, 1963.

COUNTING CONDORCET DOMAINS

GEORGINA LIVERSIDGE
(SUPERVISOR: MARSTON CONDER)

A Condorcet domain on a set A is a collection of linear orders, which has an acyclic majority relation. M.J Condorcet [3] showed that this is equivalent to the absence of the so-called *Condorcet triple* $a_1 \succ_1 a_2 \succ_1 a_3$, $a_2 \succ_2 a_3 \succ_2 a_1$, $a_3 \succ_3 a_1 \succ_3 a_2$. Defining $V(A)$ to be a set of $|A|$ vertices labelled with the elements of A, a linear order can be viewed as a directed Hamilton path on $V(A)$, giving a natural bijection between domains on A and collections of directed Hamilton paths on $V(A)$.

A Black's single-peaked domain[2] is a Condorcet domain with "peaks" along a "societal axis". An Arrow's single-peaked domain [1] is similarly defined but with the societal axis only imposed on each triple in A, which corresponds to a "never bottom" element of the triple. As such, every Black's single-peaked domain is an Arrow's single-peaked domain, but the converse is not true. Given a set A of size m, up to isomorphism there is only one maximal Black's single-peaked domain on A, however the same can not be said for maximal Arrow's single-peaked domains. The question is, how many are there?

Every maximal arrow's single-peaked domain has two terminal vertices, and two extremal paths, that is a directed Hamilton path from one of the terminal vertices to the other[4]. It was recently conjectured by A. Slinko [4] that up to isomorphism there is only one maximal Arrow's single-peaked domain for any pair of extremal paths on A.

In this talk I prove that Arrow's single-peaked domains are not defined by their extremal paths. I enumerate the number of distinct maximal Arrow's single-peaked domains for $|A| = 5, 6, 7$, and prove some results which assist with the enumeration of these objects.

References

[1] Kenneth J Arrow. *Social choice and individual values*, volume 12. Yale University Press, 2012.

[2] D. Black. On the rationale of group decision-making. *Journal of Political Economy*, 56:23–34, 1948.

[3] M. J. Condorcet et al. *Essai sur l'application de l'analyse à la probabilité des décisions rendues à la pluralité des voix*, volume 252. American Mathematical Soc., 1972.

[4] A. Slinko. Arrow's single-peaked condorcet domains. University of Auckland Algebra and Combinatorics Seminar, 2019.

Classification of ideal secret sharing schemes

Songbao Mo
Supervisor: Arkadii Slinko

Secret sharing schemes, first introduced by Shamir [2] (1979) and also independently by Blakley [1] (1979), are now widely used in many cryptographic protocols as a tool for securely storing information that is highly sensitive and important. Such information includes decryption keys, missile launch codes, and numbered bank accounts.

A *secret share scheme* is a method to distribute *share* of a secret value among a set of participants. Only the *qualified* subsets of participants can recover the secret value from their shares. The family of all qualified subsets form the *access structure* of the schemes. The scheme is *perfect* if the unqualified subsets know nothing about the secret value whatsoever. A perfect secret share scheme is *ideal* if the length of every share is the same as the length of the secret. Ideal secret sharing schemes are the most informationally efficient which is important in applications. The central problems of the theory of secret sharing schemes is to classify all access structures that can carry an ideal secret sharing scheme. The problem appears to be very difficult and only be successfully solved in some subclasses of schemes.

In this talk I will be giving a brief introduction in secret sharing schemes and discussing the notion of *framing* which occurs when a coalition (subset) is able to calculate the share of a participant who does not belong to it. Our work together with Yvo Desmedt and Arkadii Slinko shows that, in an ideal secret share scheme, an authorised coalition cannot frame participants who are less senior than all members of the coalition and it is able to frame a participant who is more senior than at least one member of the coalition.

References

[1] G.R Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings.* **48** (1979) 313-317.

[2] A. Shamir. How to share a secret. *Commun. of the ACM* **22** (1979) 612-613.

State Estimation of the Size Distribution and Underlying Physical Processes of Aerosols

Vincent Russell

Supervised by Professor Jari Kaipio

Abstract

Aerosols, a system of solid or liquid particles in a gas, are a harmful form of air pollution that play a key role in climate change and public health. To understand its effects, it is paramount to study its size distribution, which in turn is dependent on the physical processes of condensation growth, coagulation, nucleation, and deposition. These processes drive the time-evolution of the size distribution of aerosol populations. Measurements of the size distribution are obtained using a differential mobility particle sizer, however there are no direct measurements on the physical processes mentioned above. The simultaneous estimation of the size distribution and these physical processes based only on measurements of the size distribution is a *non-stationary ill-posed inverse problem.* We use the state estimation framework to simultaneously estimate the size distribution and the physical processes of condensation growth, nucleation, and deposition. Specifically, we use the extended Kalman filter as an estimator, which requires the development of a model for the time-varying size distribution and processes, and a model to relate the measurements to the size distribution and processes. We use the general dynamic equation of aerosols to model the time evolution of the size distribution which is based on the physical processes of condensation growth, coagulation, nucleation, and deposition. This is a integro-partial differential equation that is nonlinear with respect to the size distribution. We use the Petrov-Galerkin finite element method to obtain approximate solutions of the size distribution based on the general dynamic equation. We also use the method of characteristics combined with the finite element method to obtain approximate solutions. To model the evolution of the underlying physical processes of condensation growth, nucleation, and deposition, we use random walk and autoregressive processes. These models were tested with simulated measurements and obtained feasible estimates. The main contribution of this research is showing that state estimation is a feasible framework for estimating the size distribution of aerosols and the underlying physical processes, and in particular, the extended Kalman filter is a feasible approximation to the sequential filtering problem.

EMERGENCE OF CHAOTIC DYNAMICS IN AN UNBALANCED DICKE MODEL

Kevin C. Stitely[1,2,3*], Andrus Giraldo[1,3], Bernd Krauskopf[1,3], and Scott Parkins[1,2]

[1]The Dodd-Walls Centre for Photonic and Quantum Technologies, New Zealand
[2]Department of Physics, University of Auckland, New Zealand
[3]Department of Mathematics, University of Auckland, New Zealand

We study a model of the collective behaviour of N two-level atoms interacting coherently with a single mode of the radiation field - the Dicke model. In this work we study a generalised form of the model which features unbalanced coupling, $\lambda_- \neq \lambda_+$, between the rotating and counter-rotating terms of the Hamiltonian. The model takes the form of an open quantum system with cavity decay rate κ, modelled by a master equation in Lindblad form. The Hamiltonian is (with $\hbar = 1$)

$$H = \omega a^\dagger a + \omega_0 J_z + \frac{\lambda_-}{\sqrt{N}}\left(aJ_+ + a^\dagger J_-\right) + \frac{\lambda_+}{\sqrt{N}}\left(aJ_- + a^\dagger J_+\right),$$

where a is the annihilation operator of the radiation field mode, $J_\pm$, J_z are collective angular momentum operators for the atomic states, ω is the frequency of the radiation field mode, and ω_0 is the frequency splitting of the atomic levels.

In the thermodynamic limit $N \to \infty$, the model is described by a set of nonlinear ordinary differential equations,

$$\begin{aligned}
\dot{\alpha} &= -\kappa\alpha - i\omega\alpha - i\lambda_-\beta - i\lambda_+\beta^* \\
\dot{\beta} &= -i\omega_0\beta + 2i\lambda_-\alpha\gamma + 2i\lambda_+\alpha^*\gamma \\
\dot{\gamma} &= i\lambda_-\left(\alpha^*\beta - \alpha\beta^*\right) + i\lambda_+\left(\alpha\beta - \alpha^*\beta^*\right),
\end{aligned}$$

where $\alpha = \langle a\rangle/\sqrt{N} \in \mathbb{C}$, $\beta = \langle J_-\rangle/N \in \mathbb{C}$, and $\gamma = \langle J_z\rangle/N \in \mathbb{R}$.

Our work focusses on the dynamics of these equations under changes in the coupling strengths λ_- and λ_+. In particular we study phase transitions between normal phases that feature zero photon number, $\alpha = 0$, at equilibrium to superradiant phases ($\alpha \neq 0$), and transitions to oscillatory phases. These phase transitions have been experimentally realised in [1]. In the theoretical model we find superradiant phase transitions manifest themselves as pitchfork and saddle-node bifurcations, with multistability and hysteresis possible. We find the oscillatory phase transition arises from Hopf bifurcations, where superradiant phases transition to oscillatory phases with a stable limit cycle. After the Hopf bifurcation, oscillations are initially simple, nearly sinusoidal oscillations. We find these oscillations can become much more complicated under a period-doubling bifurcation, where the limit cycle splits. The system can then undergo a period-doubling cascade, with an infinite number of period-doubling bifurcations signifying the system's descent into chaos, illustrated in Fig. 1 below. We also find another chaotic attractor emerge from a Shil'nikov type homoclinic bifurcation, and then the death of oscillatory phases in other homoclinic bifurcations.

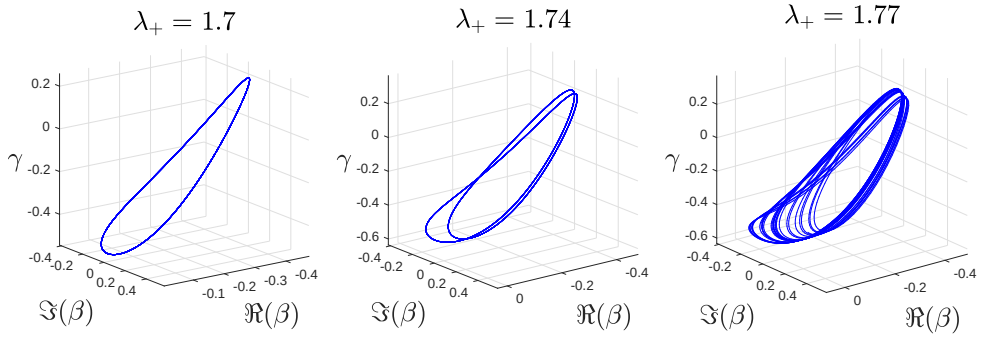

Figure 1: A period-doubling cascade on the Bloch Sphere. Here $\kappa = \omega = \omega_0 = \lambda_- = 1$, the initial condition is perturbed from the South Pole of the Bloch Sphere, $(\alpha, \beta, \gamma) = (0.001, 0.001, -0.5 + 0.001)$.

References

[1] Z. Zhiqiang, C. H. Lee, R. Kumar, K. J. Arnold, S. J. Masson, A. S. Parkins, and M. D. Barrett, "Nonequilibrium phase transition in a spin-1 Dicke model" *Optica* **4** 424-429 (2017)

*Contact email: ksti263@aucklanduni.ac.nz

Elliptic operators with Neumann boundary conditions

Chris Wong
Supervisor: Tom ter Elst

Consider a pure second-order elliptic operator

$$A = -\sum_{k,l=1}^{d} \partial_k c_{kl} \partial_l$$

on an open set $\Omega \subset \mathbb{R}^d$ with $C^{1+\kappa}$-boundary, where c_{kl} are bounded, Hölder continuous, complex valued and elliptic, subject to Neumann boundary conditions. We shall show that the semigroup generated by $-A$ has a kernel which is differentiable and that its derivatives satisfy Gaussian bounds and Hölder continuous Gaussian bounds.

In this talk, we will present a proof for the above results using tools like Morrey and Campanato spaces. We also discuss similar results when A contains lower order terms.

Connections between saddle periodic orbits as organising centres of complicated dynamics

Name: Nelson Wong
Supervisors: Bernd Krauskopf, Hinke Osinga

Connections between saddle objects, such as saddle equilibria and/or saddle periodic orbits, can be organising centres of complicated dynamics. A classical example occurs in the three-dimensional Lorenz system; connections between the origin and a pair of saddle periodic orbits mark the emergence of the well-known Lorenz attractor [1]. Such connections generally imply the existence of other interesting objects. Since these connections cannot be expressed analytically, advanced numerical methods must be developed and used to find and study them. In this talk, we shall present an example of a non-structurally stable connection between two saddle periodic orbits in an intracellular calcium model [2]; other interesting orbits that can be found nearby shall be discussed, including my recent discovery of a new non-structurally stable connection between a periodic orbit and its own period-doubled orbit.

References

[1] Eusebius J. Doedel, Bernd Krauskopf, Hinke M. Osinga. Global organization of phase space in the transition to chaos in the Lorenz system. *Nonlinearity*, 2015, 28 (11) : R113-R139.

[2] Wenjun Zhang, Bernd Krauskopf, Vivien Kirk. How to find a codimension-one heteroclinic cycle between two periodic orbits. *Discrete & Continuous Dynamical Systems - A*, 2012, 32 (8) : 2825-2851.

Classification and construction of semisimple Lie algebras

Ian Xiao
supervised by Dr. Jeroen Schillewaert

May 2019

A Cartan subalgebra of a semisimple Lie algebra is a maximal abelian subalgebra which only contains semisimple elements. A semisimple Lie algebra is a direct sum of a Cartan subalgebra with finitely many eigenspaces, each corresponds to a unique element in the dual space of the Cartan subalgebra, which we call a root. The set of roots of a semisimple Lie algebra forms a geometric object in a real inner product space satisfying certain properties, which we call a root system. We can classify root systems by Dynkin diagrams.

This classification depends on the choice of the Cartan subalgebra; however when the ground field is complex, the automorphism group of the Lie algebra acts transitively on the set of Cartan subalgebras [1]. In this talk we will show that the classification of complex semisimple Lie algebras is well-defined by providing an explicit construction of a root-space isomorphism.

In 1966 Tits [2] published a formula which takes as input two composition algebras over a given field, and ourputs a semisimple Lie algebra belonging to one of the ten families classified by Dynkin diagrams. The formula is a direct sum of various derivation algebras and Jordan algebras, endowed with a non-intuitive Lie bracket; making sure that the formula works and providing a concrete example is an extremely non-trivial task. I will give an explicit description of the formula and discuss the proof strategy involved.

References

[1] M. C. Thompson. *On the conjugacy theorem of Cartan and Borel subalgebras.* https://etd.auburn.edu/bitstream/handle/10415/2098/thesis40.pdf?sequence=2

[2] J. Tits. *Algèbres alternatives, algèbres de Jordan et Algèbres de Lie exceptionnelles.*
I. Construction, Nederl. Akad. Wetensch. Proc. Ser. A 69 = Indag. Math. 28 (1966), 223-237.

Correcting Public and Private Errors

Lukas Zobernig
Supervisor: Steven D. Galbraith

Error correction codes were first introduced by Richard Hamming in 1950. They are a method to encode data sent over unreliable or noisy communication channels [1]. The encoding process adds a certain *redundancy* to the data which is later used by the decoder to detect and (hopefully) correct possible transmission errors.

The *Hamming distance* $d_H(x, y) := \#\{i \,|x_i \neq y_i\}$ gives the distance of two binary strings $x, y \in \{0,1\}^n$ of some length $n \in \mathbb{N}$. A *linear* error correction code is called an $[n, k, d]$-code if k-length inputs result in n-length *codewords* such that the minimum Hamming distance between any codeword is d.

All of the aforementioned is concerned with correcting *public errors*, i.e. when the encoded data is given as plaintext. In this talk we will describe how to use $[n, k, d]$-codes to correct *private errors*, at least when a reasonably d_H-close guess is given [2]. We will present a new cryptographic construction based on what we call the *modular subset product problem* that allows us to *obfuscate* Hamming distance testing [3]. We will see how these techniques allow us to secure *biometric matching* such as fingerprint detection for example and also work around spelling mistakes in passwords.

Finally, we will conclude with a short outlook on our hunt for better error correction codes based on lattices [4].

References

[1] R. W. Hamming, "Error detecting and error correcting codes," *The Bell System Technical Journal* **29** no. 2, (April, 1950) 147–160.

[2] Y. Dodis and A. Smith, "Correcting errors without leaking partial information," in *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pp. 654–663, ACM. 2005.

[3] S. D. Galbraith and L. Zobernig, "Obfuscated fuzzy hamming distance and conjunctions from subset product problems." unpublished, 2019.

[4] L. Ducas and C. Pierrot, "Polynomial time bounded distance decoding near minkowski's bound in discrete logarithm lattices," *Designs, Codes and Cryptography* (2018) 1–12.