



Institute of
mathematics
& its applications

7th IMA Conference on Mathematics in Defence and Security

Abstract Book

Table of Contents

1- Mathematical challenges in security- R Pinch	3
2- Five mathematical challenges for future defence AI -K Hermiston	4
3- Evaluating understanding in AI systems- R Burnell	5
4-Using a Deep Boltzmann Machine for Reinforcement Learning in Cyber Defence - D Kent	6
5- Mathematics, Artificial Intelligence and Us – learning to work together - R Craddock	7
6-Geometrical Approaches to over the horizon radar - H Hicks, A Shibu	8
7- Variety Dynamics for taking control of complex Defense and Security contexts- T Love	9
8- What is the Density of a Chirp Statistics for Swept Frequency Signal Detection- C OBrien	10
9-Behavioural Analytics Mathematics of the Mind- R Lane	11
10- STOAT - An alternative modelling method and model for analysis and decision making- P Donnelly	12
11- MIDAS (Maximum Information Data Acquisition Strategies) for optimal observe orient- C Watkinson	13
12- A Multilayer Approach to Sanction Effectiveness with Transport Considerations- T Willis	14
13- Defence and Security - T Watson	15
14- Detecting and quantifying symmetry in large real-world hypergraphs - R.J Sanchez-Garcia	16
15- Autonomous Navigation of Unmanned Aerial Vehicles (UAVs) for Border Patrolling- B Biskin	17

Mathematical challenges in security

Richard Pinch

Abstract: In this talk I will describe how modern defence and security needs pose new challenges and how mathematics and mathematicians are meeting those challenges. I will look at two aspects of digital security. Firstly, how the imminence of practical quantum computing is changing our view of information security; secondly, some of the risks and rewards of machine learning.

Five Mathematical Challenges for Future Defence AI

Hermiston K.

kjhermiston@dstl.gov.uk, Defence Science and Technology Laboratory, UK.

Abstract

The UK Ministry of Defence has set bold and ambitious objectives as it embraces Artificial Intelligence (AI) towards achieving advantage for its operations in a changing, complex and open world. It is presently advancing its adoption of second generation AI, based largely on the experimental successes of statistical machine learning. However, Defence also seeks to understand what lies ahead for AI. This is a ‘call to arms’ mobilisation for the mathematical community. We need mathematics to not only reverse engineer the experimental successes of the current generation AI technology, towards explanation and informed design, but to take the lead in the drive to the future of AI. We need pure and applied mathematics to take the lead and stretch in answering barrier questions to transitioning AI into its next generation of capability. This is an opportunity and a challenge to the mathematical community. Can we creatively rise to that challenge? Despite well-publicised AI successes, we are at an early stage of AI definition, understanding and application but we are moving quickly. Mathematical (deterministic) and statistical (random) theory should confidently shape and drive that advance.

In this talk, we will discuss some intriguing challenges that IMA members may wish to consider and advance. There is no monopoly on good ideas. Defence needs bold, audacious and disruptive leaps of creative advance from creative minds in the mathematical community. No longer is incremental research sufficient in the Defence domain, where the threshold of adversary access to AI science and technology is low.

Evaluating understanding in AI systems

^{1*}Burnell, R, & ^{2,3,4,5}Cohn, A. G.

*lead presenter

¹rb967@cam.ac.uk, University of Cambridge, UK

²The Alan Turing Institute, UK

³University of Leeds, Leeds, UK.

⁴Tongji University, China.

AI systems are becoming ever more ubiquitous including in defence and security. Ever since researchers started building AI systems, they have wanted to evaluate them, against both human benchmarks (such as human expert chess players) and against other AI systems. The need for this just as great in the area of defence and security. Robust evaluation is vital for our ability to predict and explain the behaviour of AI systems, and to determine where and when they are safe to deploy. However, finding good benchmarks for evaluating systems is incredibly challenging—especially as systems become more general purpose.

E.g., language models such as ChatGPT are capable of performing a wide array of tasks, from answering questions about the world to writing mathematical proofs. Despite these impressive capabilities, many have questioned whether these models really *understand* the text they generate, pointing to the glaring errors the models sometimes make on tasks that seem trivial for most humans. However, the question of understanding is difficult to answer, because there is a distinct lack of clarity in these discussions about what it actually means for an AI system to understand.

We review existing ways of evaluating AI text understanding and propose novel ways in which these might be adapted to improve evaluation and develop a clearer definition of understanding. A wide variety of methods have been employed, including MCQs about specific concepts or topics, essay-style questions, and extended interviews. Another common approach attempts to infer understanding based on a system’s ability to complete certain tasks, such as to solve a problem, construct a proof, or perform some calculation. We discuss the strengths/weaknesses of these different approaches and highlight alternative methods that have so far been neglected. Ultimately, no single method of evaluating understanding is likely to be sufficient, so complementary approaches are needed.

Using a Deep Boltzmann Machine for Reinforcement Learning in Cyber Defence

¹*Kent, D., ¹O'Rourke, C., ²Bedford, A., ¹Kennedy, S., ¹Revell, A., ³Keens, R. & ³Till, S.

*lead presenter

¹d.kent@fnc.co.uk, Frazer-Nash Consultancy, United Kingdom

²Oxbrdgrbt, United Kingdom

³Dstl, United Kingdom

Cyber attacks are becoming more sophisticated and increasingly automated, often outpacing defenders. Autonomous cyber defence systems potentially provide a means to reduce the time taken to respond to incidents. There is significant interest amongst the research community on the application of Reinforcement Learning (RL) in this space. Training RL systems requires data that is not easily captured, and often there is insufficient data to train a RL agent in a classical manner. Quantum hybrid methods offer a potential route to extract greater learning and insight from limited data. Early research has indicated that in other areas of Machine Learning (ML), such as image classification, quantum systems may learn faster. However, due to the challenges of device access, few experiments have managed to fully train models, making the comparison challenging.

In general, Quantum Machine Learning (QML) is in its infancy and its benefits have yet to be realised. Whilst the growth in qubit number, connectivity and capability of quantum devices is rapid and promising, the current devices are limited. Furthermore, accessing quantum devices in a timely manner is difficult, with queuing for access common.

Frazer-Nash Consultancy and Oxbrdgrbt have collaborated with Dstl to test the benefits of QML in a cyber defence environment, specifically looking to answer:

“By using a quantum hybrid Deep Boltzmann Machine (DBM) approach on a D-WAVE, can a RL agent be trained, to a similar accuracy, with fewer data points, than by a classical approach?”

The research uses the cyber defence framework YAWNING-TITAN [1] to provide testing in a controlled environment. The DBM approach requires optimal and near-optimal solutions of Quadratic Unconstrained Binary Optimisation problems, or equivalently, low energy states of an Ising model, which the D-WAVE device is designed to return.

The presentation will discuss the effectiveness of the method compared to classical methods, and discuss the challenges posed by the approach and future avenues for exploitation.

1. <https://github.com/dstl/YAWNING-TITAN>

Mathematics, Artificial Intelligence and Us – learning to work together

Rachel Craddock

Many forms of Artificial Intelligence rely on mathematics. It facilitates the development and use of AI and machine learning. Historically, mathematics enabled the growth of many forms of AI, such as neural networks developing from simple human tuneable networks to complex networks requiring machine learning. Mathematics also forms the interface between humans and many forms of AI. It is used to capture and represent our requirements, to assess the quality of the AI solutions and to enable us to train complex AI solutions. This interface is also where many of the issues with modern AI stem from. One of the big issues is will the AI work as desired when required? Mathematics can help us to determine the answer to this question, and enable us to work successfully with AI. This presentation will describe how mathematics is used in AI, and how it can help us to determine if AI is meeting our requirements.

Geometrical Approaches to Over the Horizon Radar Modelling

¹Andrew Ash, ²*Harry Hicks & ³*Allen Shibu.

*lead presenter

The UK military has a wide range of requirements related to the detection, identification and tracking of objects at long ranges to support a variety of missions. The use of radar is well established, however the majority of systems are constrained by line of sight (LOS) geometry that limits the ranges at which targets can be detected. In contrast Over The Horizon Radar (OTHR) has the capability to detect targets beyond LOS coverage, hence increasing available time to detect targets at range. SkyWave OTHR exploits the ionosphere, the cold weakly ionised region around the Earth caused by solar radiation incident on the atmosphere. As this region depends on several highly variable processes (solar activity, atmospheric variations, interactions between different gas species etc.) OTHR performance is highly variable. This has important consequences when considering its military utility that (in general) require sensor systems that can operate 'on demand'.

This paper describes the methodology developed within Dstl SSG to assess the military utility of OTHR in a number of scenarios. In particular, the focus is on a geometrical model to provide a measure of effectiveness for an OTHR system in terms of its ability to detect and track objects for a range of deterministic ionospheric conditions. The Flower Petal Method (FPM) developed at Dstl provides a highly efficient method of estimating the characteristics of multiple ionospheric bounces that provides significant computational savings over traditional, ray-tracing methods. A statistical measure of the expected amount of time that the OTHR will operate is provided using this method. Derivation of the geometrical calculations used to predict OTHR coverage will be provided in the paper and initial results presented. Ongoing work on the incorporation of higher fidelity ionospheric models will also be discussed.

Variety Dynamics for taking control of complex Defense and Security contexts

¹*Love, T, ²Cooper, T.

*lead presenter

¹admin@loveservices.com.au, Love Services Pty Ltd, Western Australia

²Edith Cowan University, Western Australia

Variety Dynamics is a new mathematically based approach for taking control of highly complex and hyper-complex Defense and Security situations including in terrorism, asymmetric warfare, information warfare, intelligence, and the cyber-physical realms.

The primary focus of Variety Dynamics is to change the ownerships, dynamics and trajectory of control in highly and hyper complex situations. It is especially well suited to successful decision making in situations for which conventional systems assumptions and causal modelling do not apply or are too difficult or too slow to apply.

Unlike almost all other mathematical or strategic approaches to decision support for Defense and Security it does not require or use information about causal relationships. It addresses strategic decision-making and management of control of complex coercive situations in a different way.

The different approach of Variety Dynamics means its influences are intrinsically covert and due to the 2 Feedback Loop Axiom are typically invisible to other parties.

Variety Dynamics also addresses key problems in control of hyper-complex non-linear multi-feedback loop control systems and provides a theoretical foundation for more computationally efficient approaches to AI modelling.

Our work on Variety Dynamics has been developed and tested over the last 20 years. Aspects of Variety Dynamics have been presented in variety of conferences venues including the recent International Systems Sciences Conference in Johannesburg. A paper on Variety Dynamics is in preparation for the Journal of Information Warfare and a book is under discussion with Routledge.

The presentation will describe the basics of Variety Dynamics and provide a sample of practical examples and outline the over 45 axioms for effective decision making to obtain control of highly complex and hyper-complex situations typical of Defense and Security.

What is the Density of a Chirp?

Statistics for Swept Frequency Signal Detection

Cian O'Brien

Chelton Limited, The Chelton Centre, Fourth Avenue, Marlow SL7 1TF. United Kingdom.
cian.o'brien@chelton.com

Chirp, frequency modulated, or swept frequency signals play a vital role in various signal processing applications including system response measurement, pulsed Doppler radar design, chirp spread spectrum systems and, significantly, the antagonistic jamming of the Global Positioning System (GPS). In this work, we investigate signals resulting from uniform random samplings of periodic and continuous chirp signals and demonstrate that they can be characterized by a family of probability distributions with two parameters. The first parameter corresponds to the type of frequency sweep (e.g. constant, linear or quadratic), while the second parameter is related to the time-frequency product of the chirp. We provide expressions for the probability density function and cumulative distribution function of random samplings of continuous periodic chirps and explore some of their limiting behaviors.

Next, we propose an entirely time-domain algorithm for detecting chirp signals by utilizing the derived distributions as part of a one-sample hypothesis test. The prevalence of affordable and portable chirp jammers poses significant concerns for aircraft navigation and autonomous driving and consequently there is a pressing need for algorithms that can detect, classify and otherwise mitigate adversarial signals. As a practical application, we therefore focus on the detection of jamming attacks which aim to disrupt satellite reception and impede GPS acquisition through the transmission of nuisance chirps over the targeted frequency band. To evaluate the effectiveness of the proposed algorithm, we conduct a simulation using signals with chirp parameters chosen based on those found in a range of commercial jamming devices.

Behavioural Analytics: Mathematics of the Mind

¹*Lane, R.O., State-Davey, H.M., Taylor, C.J., Holmes, W.J., Boon, R.A. & Round, M.D.

*lead presenter

¹rlane1@qinetiq.com, QinetiQ, UK

Behavioural Analytics provides insights into individual and crowd behaviour, enabling analysis of what previously happened and predictions for how people may be likely to act in the future. In defence and security, this allows organisations to achieve tactical and strategic advantage through influence campaigns, a key counterpart to physical activities. Before action can be taken, online and real-world behaviour must be analysed to determine the level of threat. Huge data volumes mean that automated processes are required to attain an accurate understanding of risk.

Recent developments in large language models enable the encoding of online statements into high-dimensional vector embedding representations. Embeddings from each statement by an individual can be considered to be a noisy measurement of their state of mind. Sequences of statements can be processed to provide not only more accurate estimations at any point in the past but also predictions about the likely trajectory of thought, with associated uncertainty measures. These predictions can be used to assess the probability of extremist activities.

We describe the mathematical basis of technologies behind a system to analyse quotes in multiple languages. These include a Bayesian network to understand behavioural factors, state estimation algorithms for time series analysis, and machine learning algorithms for classification.

We present results from studies of quotes in English, French, and Arabic, from anti-violence campaigners, politicians, extremists, and terrorists. The system correctly identifies extreme statements; and analysis at individual, group, and population levels detects both trends over time and sharp changes attributed to major geopolitical events. Group analysis showed that additional population characteristics can be determined, such as polarisation over particular issues and large scale shifts in attitude. Finally, MP voting behaviour and statements from publically available records are analysed to determine the level of correlation between what people say and what they do.

STOAT - An alternative modelling method and model for analysis and decision making

Donnelly, P., Emery, T., Pickford, G., Ash, A., Dodd, C.

rpdonnelly@dstl.gov.uk

Dstl Strategic Systems, Portsmouth West, UK

The use of mathematical models for analysis and assistance in decision making is widespread in research, industry and government. Models vary in complexity of representation and data and modelling can be performed at different levels of abstraction. Models are expensive to develop, assure and maintain so are frequently applied to a number of problems, some not necessarily in the original requirements scope. In usage similar problems emerge in models across all levels and applications, these include lack or inconsistency of data sets at the required level of detail, hidden assumptions and constraints, understanding of the uncertainty of outputs. Monte-Carlo modelling is frequently used to determine the risk and impact of random variables prediction and forecasting but is costly in computing time and complexity.

Our specific problem domain involves assessing complex architectures of interacting systems in various scenarios, frequently information on particular systems is not fully available and specific analysis is needed in constrained time scales. An alternative approach and method of modelling has been investigated and developed. This defines, generates and evaluates the probabilities of possible chains of events that can happen in the scenario. Probabilities may come from a variety of sources, detailed models, design information, subject matter expert opinion etc. and so uncertainties can be identified.

In realistic situations the chains of objects in scenario, events and numbers of evaluations needed grow exponentially and become practically intractable. By implementing set operators and nuanced rules to determine event occurrence and using combinations rather than permutations for branching, together with a 'dispatcher' function to allow user choice of which branches to evaluate, it has been found that the model can run quickly with known coverage. Comparisons to existing models have shown good correspondence and also indicate potential for wider applications and to address other issues associated with conventional modelling approaches.

MIDAS (Maximum Information Data Acquisition Strategies) for optimal Observe-Orient-Decide-Act loops

^{2,3}Handley, W. J., ^{2,3}Hobson, M. P., ^{1,2}McAloon, T & ^{2*}Watkinson, C. A.

*lead presenter

¹thomas.mcaloone@polychord.co.uk

²PolyChord Ltd, 27 Mortimer Street, London, W1T 3BL

³Kavli Institute for Cosmology, University of Cambridge, Cambridge, CB3 0EZ

In this talk we will present the MIDAS (Maximum information data acquisition strategies) optimisation framework for machine-assisted decision support, the development of which was supported by the Defence Science and Technology Laboratory (DSTL). MIDAS is a mathematical expression of the classic military Observe-Orient-Decide-Act loop that can be used to decide which of a set of possible next steps, or strategies, will be most effective given the current state of knowledge. It makes predictions of the expected information gain given a targeted exploration of all the possible solutions to the problem being solved, and all the possible datasets one could collect under a particular strategic choice. Given such metrics for a set of strategies, one may then pick the one with the best average information gain. Equally a human-in-the-loop decision maker can be given full information as to the distribution of predicted information gain each strategy might return, in order to augment their decision making. This framework can also be applied to mission planning, allowing the user to play out possible strategies in advance of engagement. We will present some examples of the kind of problems that this approach has historically been applied to, including locating transmitters in a cityscape, detecting star networks, controlling multi-purpose drones in order to deactivate an opponent's base station. In doing so, we will demonstrate that these techniques are beginning to be applicable now to a wide range of problems using modern computing power, and are suitable as a generation-after-next technology for optimally synthesising information and making semi-automated decisions in an interpretable and robust fashion.

A Multilayer Approach to Sanction Effectiveness with Transport Considerations

¹*Willis T.E., ¹Punzo, G.

*lead presenter

¹tewillis1@sheffield.ac.uk, University of Sheffield, United Kingdom

Sanctions and trade embargoes are key tools in international security. The underlying principle from a game theoretic perspective is leveraging soft power to disincentivise defection from international norms by increasing the cost of doing so. This results in further costs for both countries that impose sanctions as well as those on whom sanctions are imposed. Where countries imposing sanctions can demonstrate that they are committed to sanctions and will impose them in each case, and that the sanctions cause a significant reduction in the defector's utility, the regularity of sanctions being required decreases as instances of international defection are reduced. The incentive for the target to attempt to bypass the sanctions is therefore clear, allowing them to take their preferred course of action. The problem of maximising the effectiveness of sanctions can be approached by creating a model to predict the effectiveness of sanctions and understand the process of export-deflection. This work introduces a Bi-Layer model of single homogeneous commodity international trade. The first layer is of supply and demand, and the second of transport costs. The stable equilibria are found for the model before and after sanctions occur, and the resultant change between them can be used to examine the total utility cost to the countries of imposing sanctions. The model is shown to mirror real-life conditions such as the increased utility of a sanctioned player when multiple options for sanction bypass are available to them through the Shapley value of the players. The result of increasing the number of sanctioned players to include those who are otherwise incentivised to assist the defector for their own benefit is demonstrated, as well as the loss of effectiveness of sanctions when one or more sanctioning player chooses not to impose sanctions.

Professor Tim Watson, Programme Director for Defence and Security at The Alan Turing Institute

¹*Professor Tim Watson

*lead presenter

Professor Tim Watson will briefly cover the history and context of the Turing Institute and the Defence and Security Programme within it. He will then outline the development of the next phase of Turing (Turing 2.0) and describe the missions within the new grand challenge for Defence and Security and how researchers can contribute to this work.

Detecting and quantifying symmetry in large real-world hypergraphs

¹Pritchard, Y. & ^{1,2*}Sanchez-Garcia, R.J.,

*lead presenter

¹R.Sanchez-Garcia@soton.ac.uk, Mathematical Sciences, University of Southampton, UK

²The Alan Turing Institute, UK

Hypergraphs can represent complex higher-order interactions in data, in contrast to graphs (networks), which are limited to pairwise interactions between data points. There is an increasing availability of hypergraph data sets and one natural question is to quantify the amount of structural redundancy present in such data. For real-world complex networks, for instance, it has been shown that they exhibit a large number of relatively simple symmetries, generated at small subgraphs called symmetric motifs. In this work, we describe an efficient algorithm for the detection and quantification of symmetries on an arbitrary hypergraph, and show that many real-world hypergraphs exhibit a large number of local symmetries. We study their most common types of symmetries found in real-world hypergraphs and explain how the presence of symmetries can be exploited, for instance for lossless compression, and to reduce the computational time reduction of downstream analyses. This work was carried out during a dstl research contract facilitated by the Alan Turing Institute Defence and Security Programme.

Autonomous Navigation of Unmanned Aerial Vehicles (UAVs) for Border Patrolling: A Stochastic Framework

^{1*}Busra Biskin, ¹Joerg Fliege, ¹Toni Martinez-Sykora

¹b.biskin@soton.ac.uk, CORMSIS, University of Southampton, United Kingdom

Unmanned Aerial Vehicles (UAVs) have emerged for military purposes and have been frequently used for military operations since World War II. Employing UAVs, especially in risky and complex military operations such as reconnaissance missions, espionage, and detecting and attacking targets, helps decreasing the risk of the mission and increasing the mission's speed and success rate since human fatigue is eliminated from the mission by using UAVs. In this study, we focus on employing UAVs in internal safety, i.e., border patrolling operations, which require rapid information flow, higher precision and accuracy, unlike civil applications. We develop an algorithm for a fully autonomous UAV to take its own actions, navigate itself within given constraints, and test our algorithm by simulation in case of a border violation when we develop an algorithm for automating navigation decisions of UAVs.

In the border violation incident, UAV is on the duty of surveillance and defending the area; it searches the area and pursues the intruder, aiming to detect it before the intruder passes through the border. Since, in real life, border invasions frequently happen from the same borderline repetitively, both UAVs and intruders cannot follow a deterministic strategy to be successful. Therefore, the main objective of this study is to develop an excellent stochastic strategy for aspects of UAV navigation, considering the minimization of time required to complete the mission while maximizing the probability of success of the mission where the mission includes uncertainty arising from lack of knowledge about the intruder's movement. The movement of the UAV and intruder is modelled via simulation through different scenarios, and the problem is solved using a response surface methodology: Radial Basis Function.

The developed algorithm and the model are applicable in various real-life scenarios where no information for the intruder's movement is available or just partial information can be collected. The developed mathematical tools can be used in disaster management, especially in the defense industry.