华东师范大学软件工程学院
教育部可信软件国际合作联合实验室
国家可信软件国际联合研究中心
国家软件人才国际培训基地（上海）

Formal Methods for Trustworthy Artificial Intelligence

面向人工智能系统的形式化方法

软件工程学院 SOFTWARE ENGINEERING INSTITUTE
教育部可信软件国际合作联合实验室 MOE International Joint Lab of Trustworthy Software

“Formal Methods for Trustworthy Artificial Intelligence”
SEI-Summer School 2020

Time \ Date		Monday	Tuesday	Wednesday	Thursday	Friday
		13, July	14, July	15, July	16, July	17, July
Morning	8:30-10:10	Shaoying Liu Hiroshima University	Zhiming Liu Southwest University	Shield Lab Huawei	Shaoying Liu Hiroshima University	Zhiming Liu Southwest University
	10:10-10:30	Break	Break	Break	Break	Break
	10:30-12:00	Shaoying Liu Hiroshima University	Zhiming Liu Southwest University	Shield Lab Huawei	Shaoying Liu Hiroshima University	Zhiming Liu Southwest University
Noon	12:00-14:00	Lunch	Lunch	Lunch	Lunch	
Afternoon	14:00-15:30	Xiaowei Huang Liverpool University	Xiaowei Huang Liverpool University	Guy Katz The Hebrew University of Jerusalem	Guy Katz The Hebrew University of Jerusalem	
	15:30-15:50	Break	Break	Break	Break	
	15:50-17:20	Xiaowei Huang Liverpool University	Xiaowei Huang Liverpool University	Guy Katz The Hebrew University of Jerusalem	Guy Katz The Hebrew University of Jerusalem	

Course Introduction

Formal Engineering Methods for Software Quality Assurance (Prof. Shaoying Liu)

Conventional software engineering based on informal or semi-formal methods are facing tremendous challenges in ensuring software quality. Formal methods have attempted to address those challenges by introducing mathematical notation and calculus to support formal specification, refinement, and verification in software development. However, in spite of their theoretical potential in improving the controllability of software process and reliability, formal methods are difficult to apply to large-scale and complex systems in practice due to many constraints (e.g., limited expertise, complexity, changing requirements).

"Formal Engineering Methods" (FEM) has been proposed and developed as a research area since 1997 to study how formal methods can be effectively integrated into conventional software engineering process to improve software productivity and quality in practice. A specific representative FEM called Structured Object-Oriented Formal Language (SOFL) has also be developed over the last two decades that offers three rigorous but practical techniques for system modeling and verification: three-step formal specification approach, specification-based inspection, and specification-based testing. The effective combination of these three techniques can significantly enhance software productivity and quality.

This course aims to teach students how formal engineering techniques can be effectively used in conventional software engineering process to enhance software productivity and quality through introducing SOFL. After learning this course, students are expected to understand (1) essential knowledge and skills for writing formal specifications, (2) how to construct formal specifications based on informal requirements, (3) how to balance simplicity, visualization, and precision in software development, and (7) future research directions in formal engineering methods.

Course Introduction

Prof. Shaoying Liu

刘少英是日本广岛大学教授，IEEE Fellow 和英国计算机协会（BCS）Fellow。1982 年 1 月毕业于西安交通大学，1987 年获同大学的计算机科学硕士学位，1992 年获得英国曼彻斯特计算机科学博士学位。 主要研究领域包括软件工程，软件开发的形式化工程方法，软件设计方法，程序验证，软件测试，以及智能软件工程环境。 从 1994 年以来，已领导和主持由日本文部科学省，国立信息研究所（NII），大川情报科学财团，以及日本信号， NTT Data, 和三菱电机等日本政府，财团和大企业分别资助的 20 多个研究项目，是华为和卡斯柯信号有限公司的技术顾问，创立和发展了``软件开发的形式化工程方法’’， 研制开发了 SOFL 形式化工程开发语言和方法，由 Springer 出版专著一本，编著由 IEEE CS Press 和 Springer LNCS系列出版的论文集 12 本， 在包括 IEEE Transactions on Software Engineering, IEEE Transactions on Reliability, Journal of Systems and Software等 国际学术期刊和国际会议发表 200 多篇论文。

曾被 Journal of Systems and Software评为 1993年至 1996年期间的在系统和软件工程领域的世界 top 15名学者之一，1996 年获得由 IEEE 国际会议授予的``优秀论文奖’’， 2011 年 10月获中国国家示範软件学院十佳兼職教師奨，2017 年 6 月获得IEEE 可靠性协会日本分会的 2016 年最佳论文奖。曾多次担任ICFEM，ICECCS 等国际会议的大会主席和程序委员会主席，以及数目繁多的国际会议的PC 委员，被欧，美，亚，奥等地区的 60 多个大学和研究机关以及国际会议邀请作学术报告，曾担任Software Testing，Verification and Reliability (STVR)学术期刊的 Associate Editor。 现任 IEEE Transactions on Reliability的Associate Editor以及 International Journal of Intelligent Internet of Things Computing 的Advisory Board 成员。

Course Introduction

Software Abstractions and Human-Cyber-Physical Systems Architecture Modelling (Prof. Zhiming LIU)

Human-Cyber-Physical Systems (HCPS) is a combination of Cyber-Physical Systems (CPS) with ubiquitous computing (also known as intelligent environment) and social systems, including social computing. In HCPS, humans as individuals or unorganized and organized crowds deeply involved in interactions with physical and cyber systems, and operation and control of physical processes and hardware dynamically shift between humans and machines. The theory and methods of HCPS is still in its infancy, and research is needed to establish its scientific foundation so as to make advances in its engineering methods.

In this short course, we reflect the development of software engineering through software abstractions and show that these abstractions are integral in the notion of software system architectures. We discuss that it is important to engineer systems using formal methods in relation to the definition and management of development processes, and argue how a model of the software architecture, with rich semantics and refinement relations, plays an important role in this process. We recall the traditional separation of processes for domain modelling and software requirements modelling in model-driven software development. We then propose to combine these modelling approaches and this naturally leads to a unified process for HCPS architecture modelling, design, and evolution. Based on the unified processes, we outline a framework in engineering formal methods for HCPS modelling, with the discussion about significant challenges including integration, composition, collaboration, verification of HCPS with multi-dimensional heterogeneity. Human components, as well as all kinds of artificial intelligent systems, are particularly major courses of the heterogeneity.

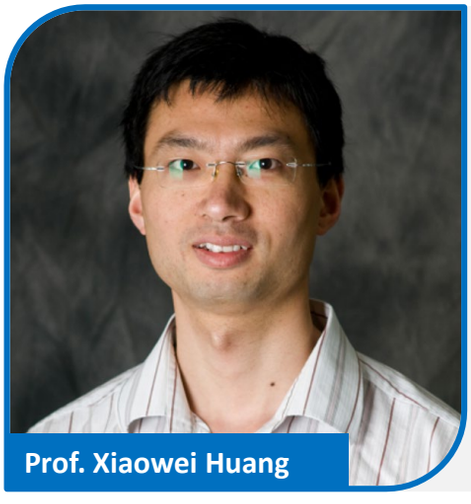
Prof. Zhiming LIU

Zhiming LIU has been working in the area of software theory and methods. He is known for his work on Transformational Approach to Fault-Tolerant and Real-Time Systems, Probabilistic Duration Calculus for System Dependability Analysis, and rCOS Method for Object-Oriented and Component-Based Software. Zhiming Liu studied mathematics in university. He holds a MSc in Computing Science from Software Institute of CAS (1988) and a PhD in Computer Science from University of Warwick (1991). Zhiming Liu joined Southwest University in Chongqing as a full-time professor of computer science in 2016. He is leading the development of the University Centre for Research and Innovation in Software Engineering (RISE). Before Southwest University, he worked in three universities in the UK (1988-2005 and 2013-2015) and the United Nations University – International Institute for Software Technology (Macau, 2002-2013).

Course Introduction

Safety Certification of Deep Neural Networks (Prof. Xiaowei Huang)

Significant progress has been made in the development of deep neural networks (DNNs), which now outperform humans in several difficult tasks, such as image classification, natural language processing, and two-player games. Given the prospect of a broad deployment of DNNs in a wide range of applications, concerns regarding the safety and trustworthiness of DNNs have been raised. In this lecture series, I will review two threads of existing research towards safety certification of DNNs. The first thread is on the formal verification. In particular, I will focus on constraint-based methods, approximation techniques, and anytime algorithms. The second thread of research is on the safety assurance of DNNs through testing- based method. This is based on an established approach that has been recommended in industrial standards such as ISO26262 for automotive software and DO178B/C for avionic software, and it has been adapted for DNNs.



Prof. Xiaowei Huang

Dr Huang is currently a Reader at the University of Liverpool (UoL). Prior to UoL, he worked at the University of Oxford and the University of New South Wales in Australia. Dr Huang's research is concerned with the development of automated verification techniques that ensure the correctness and reliability of intelligent systems. His recent research on the verification of deep learning systems addresses a major concern recently raised by both the general public and the governments on the safety and robustness of deep learning systems. Dr Huang has given a number of invited talks on the trustworthiness and safety of machine learning techniques and their application to safety critical systems. He is the PI (or Liverpool PI) for projects valued more than £1.4M, and co-I for more than £15M. He is directing the VR (Verifiable Robotics) Laboratory in the Digital Innovation Facility (DIF) Building at Liverpool.

Course Introduction

Formal Verification of Deep Neural Networks (Prof. Guy Katz)

Deep neural networks have emerged as a widely used and effective means for tackling complex, real-world problems. However, a major obstacle in incorporating them as controllers in safety-critical systems is the great difficulty in providing formal guarantees about their behavior. In recent years, attempts have been made to address this obstacle by formally verifying neural networks. However, neural network verification is a computationally difficult task, and traditional verification techniques have often had only limited success - leading to the development of novel techniques. In this series of talks we will survey the state of the art in neural network verification, focusing on Satisfiability Modulo Theories (SMT) based approaches and on abstraction/refinement based methods. Additionally, we will survey recent advances in the verification of recurrent neural networks. Finally, we will discuss the applicability of neural network verification, going over examples that include airborne collision avoidance, neural network simplification, and the verification of rate control algorithms.

Prof. Guy Katz

Guy Katz is an assistant professor at the Hebrew University of Jerusalem, Israel. He received his Ph.D. at the Weizmann Institute of Science in 2015. His research interests lie at the intersection between Formal Methods and Software Engineering, and in particular in the application of formal methods to software systems with components generated via machine learning.

Course Introduction

Trustworthiness and formal verification of AI systems (Mr. Xuejun Wen & Dr. Dai, Ting)

Mr. Xuejun Wen

Mr. Xuejun Wen has got educated in Mathematics and Statistics in Peking University and Hangzhou University. He is a senior security researcher of Shield Lab which is the strategic security lab of Huawei. Before joining Huawei, he was a senior researcher of Infocomm Security Department in Institute for Infocomm Research, A*Star. Mr. Wen's research interests are in AI security and IoT security. He provided many security technologies & solutions for Huawei production lines. Meanwhile, he participated in many security security and privacy insight studies. Recently, he focuses his interest in the verifications of AI models.

Dr. Dai, Ting is a senior researcher in the Trustworthy AI Lab of Shield Lab at Huawei Singapore Research Center. He received his Ph.D. degree in Computer Science from National University of Singapore in 2015, and B.S. degrees in Computer Science from Tsinghua University in 2009. His research area is in system and software security, and security in emerging platforms, such as AI, Web, mobile, and Internet-of-things (IoT). He has been publishing research papers in top security and software engineering conferences and owns several high-value security related patents.


Dr. Dai, Ting

Course Introduction

Consider Formal Verification of Neural Network Robustness from the perspective of Huawei (Dr. Chengqiang Huang)

In this talk we will briefly discuss the current applications of formal verification of neural network robustness in Huawei. The desire features of the verification methods in industrial products will be highlighted. Some promising on-going research directions will also be discussed in the purpose of discovering new research ideas and applications of formal verification methods in the field of AI robustness.

Dr. Chengqiang Huang

Doctor Chengqiang Huang is currently a senior research engineer in Huawei. He recieved his bachelor and master degree from Xidian University in 2011 and 2014 respectively. In 2018, he recieved his doctor degree from the University of Exeter majoring in anomaly detection methods and applications. Later in 2018, he joined Huawei and since then he has been working in the field of AI robustness.