Kangfeng Ye, Ph.D.

kangfeng.ye@york.ac.uk randallye Academic Homepage RandallYe

Summary

Short — Formal verification, Formal semantics, Probabilistic programming languages, Probabilistic model checking and theorem proving, Model-based software engineering, Robotics, Tool development

Brief — In my research, I (1) use mathematical logic (alphabetised predicate calculus in Unifying Theories of Programming - UTP) to give (**probabilistic**) semantics (denotational and operational semantics) to a domain-specific language (RoboChart) in robotics, with support of modelling time and probability, (2) develop **automated verification tools** using modern model-based techniques (model transformation, validation, and generation) and formal verification (model checking and theorem proving), and (3) apply theoretical semantics and practical tools to a variety of case studies. I am a developer of RoboTool supporting formal verification for robotic application, and a contributor of Isabelle/UTP, a unifying semantic framework supporting theorem proving. Both tools are being developed in the RoboStar group.

Methodology — I usually start with the development of mathematical semantics and the definition of semantics generation rules, then implement them in tools for automated verification and validate them with case studies. Finally, the work is published and applied to verify real robots. My work is a combination of theoretical computer science with software engineering (particularly in model-based and programming).

Showcases — My recent work is summarised in two posters (probabilistic modelling and verification and formally verified animation of robotic controllers) and demonstrated (automated probabilistic verification, animation of an autonomous chemical detector controller, and a new probabilistic programming language and its verification support in theorem proving).

Industry — Before I moved to academia in 2012 to pursue a PhD, I had eight years of experience as a senior software and firmware leader in the industry: embedded systems in semiconductor equipment and high-end ToR data centre switches. I have seen major challenges in traditional software and system engineering, for example, dependability and assurance are not guaranteed. This motivated my interest in formal methods.

Employment History

- 2016.12 – ···· **Research Associate**, University of York, UK. Worked on two EU H2020 projects and four EPSRC-funded projects.
- 2012 – 2015 **Part-time Software Engineer**, Rapita Systems, York, UK.
- 2007 – 2012 **Embedded Software and Firmware Lead**, Celestica R&D Centre, Shanghai, China.
- 2004 – 2007 **Alignment Subsystem Software Lead**, Shanghai Micro Electronics Equipment, Shanghai, China.

Education

- 2012 – 2016 **Ph.D. Computer Science, University of York** in Formal Methods.
  Thesis title: *Model Checking of State-Rich Formalisms.*
  Keywords: *Formal Semantics, Formal Verification, Model Checking, Process Algebra, State-based Formalism.*
- 2001 – 2004 **M.Sc. Machine Design, Chongqing University** in Computer-Aided Design.
  Thesis title: *Levelling Control System with High Precision for Platform bearing Heavy Loads.*
  Keywords: *PID Controller, Matlab/Simulink, C Programming.*
- 1997 – 2001 **B.Sc. Machine Design, Chongqing University**.

Academic career (paradigms) - chronological order

▷ A lightweight security model checker using sound animation	The development of a lightweight model checker to verify security protocols using automatically generated sound animators, which are accessible for protocol designers.
▷ QoS analysis for Open-RAN applications	The use of probabilistic model checking to analyse energy efficiency and service availability of a control policy for Open-RAN applications.

Academic career (paradigms) - chronological order (continued)

▷ Safety Assurance of activity diagrams for systems exhibiting time and uncertainty	The development of a new comprehensive approach (1) to give annotated UML activity diagrams (with probability, time, reliability etc.) the semantics in three Markov models (DTMCs, MDPs, and CTMCs), (2) to automatically generate semantics in the PRISM language, (3) to verify generate models using probabilistic (parametric) model checking by PRISM and Storm, and also synthesise controllers.
▷ Probabilistic theorem proving	The formalisation of the new PPL in Isabelle/HOL with many proven algebraic laws. Six probabilistic programs are proven. This provides a new probabilistic semantic framework for unifying probabilistic models (such as Markov models and Bayesian networks).
▷ Probabilistic programming	A new PPL with formal mathematical semantics, capable of modelling epistemic and aleatoric uncertainty, supporting Bayesian reasoning and theorem proving.
▷ Theorem proving for RoboChart	Development of the operational semantics for RoboChart (based on CSP) and the theories in Isabell/HOL to automatically generate Haskell code for sound animation.
▷ Theorem proving for pGCL	Mechanisation of the weakest completion semantics of a probabilistic programming language pGCL in Isabelle/HOL, which enables theorem proving of nondeterministic probabilistic programs with loops and infinite state space.
▷ Quantitative property language	Specification of qualitative and quantitative properties (PCTL*) for RoboChart and the support of automation in RoboTool using model-based code generation.
▷ Probabilistic model checking for DSL (RoboChart), and Meta-model for PRISM	Semantics for probabilistic RoboChart, a DSL for graphical modelling of robotic control software, about 100 mathematical rules for semantic generation, the implementation of rules in RoboTool plugins for fully automated verification using probabilistic model checking (PRISM), which is based on model-based transformation.
▷ Theorem proving for Simulink	Creation of a new theory for Simulink concrete control diagrams and the mechanisation of the theory in Isabelle/HOL to support automated compositional contract-based reasoning.
▷ Engineering a robot	Creation of a physical and control model for a line-following robot, and the development of its co-simulation and PID controller software code (C++). It is demonstrated online here.
▷ Cyber-Physical Systems	Physical modelling, Model-based testing, and Co-simulation, in the INTO-CPS project (Integrated Tool Chain for Model-based Design of Cyber-Physical Systems).
▷ A parser and type-checker	Developed using Haskell Alex and Happy for parsing and type-checking ISO Standard Z (ISO/IEC 13568:2002) and Circus, a state-rich formalism.
▷ Model checking	My PhD thesis is about model checking of a state-rich formalism Circus (a combination of CSP and the Z notation).
▷ Embedded software (industry)	Led a team to develop embedded software and firmware for the semiconductor equipment and communication systems in two R&D companies. I have developed software for various embedded OSs: Embedded Linux (Open Source and WindRiver), VxWorks, and Bare-metal on Micro-controllers.

Awards and Achievements

2022 Software and Systems Modelling (SoSyM) Journal-First Paper Award: "Probabilistic modelling and verification using RoboChart and PRISM", invited to present it at the MODELS 2022 conference.
▷ On 16th January 2024, interviewed by Dr. Daniel Shea from Karlsruhe Institute of Technology (KIT) on the online podcast Scholarly Communication. My interview is available online here and is titled "Use Sequential Internal Review to Improve Your Next Submission".

Research Publications

Journal Articles

1. **K. Ye**, S. Foster, and J. Woodcock, "Formally verified animation for RoboChart using interaction trees," *Journal of Logical and Algebraic Methods in Programming*, vol. 137, p. 100 940, 2024, ISSN: 2352-2208. DOI: https://doi.org/10.1016/j.jlamp.2023.100940.

2. **K. Ye**, J. Woodcock, and S. Foster, "Probabilistic unifying relations for modelling epistemic and aleatoric uncertainty: Semantics and automated reasoning with theorem proving," *Theoretical Computer Science*, p. 114 876, 2024, ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2024.114876.

3. **K. Ye**, A. Cavalcanti, S. Foster, A. Miyazawa, and J. Woodcock, "Probabilistic modelling and verification using RoboChart and PRISM," en, *Software and Systems Modeling*, vol. 21, no. 2, pp. 667–716, Apr. 2022, ISSN: 1619-1374. DOI: 10.1007/s10270-021-00916-8. (visited on 10/13/2023).

4. S. Foster, **K. Ye**, A. Cavalcanti, and J. Woodcock, "Automated Verification of Reactive and Concurrent Programs by Calculation," *Journal of Logical and Algebraic Methods in Programming*, vol. 121, p. 100 681, Jun. 2021, arXiv:2007.13529 [cs], ISSN: 23522208. DOI: 10.1016/j.jlamp.2021.100681. (visited on 10/13/2023).

5. **K. Ye** and J. Woodcock, "Model checking of state-rich formalism by linking to $$CSP\,\Vert \,B$$," en, *International Journal on Software Tools for Technology Transfer*, vol. 19, no. 1, pp. 73–96, Feb. 2017, ISSN: 1433-2787. DOI: 10.1007/s10009-015-0402-1. (visited on 10/13/2023).

Conference Proceedings

1. R. Metere, **K. Ye**, Y. Gu, *et al.*, "Towards Achieving Energy Efficiency and Service Availability in O-RAN via Formal Verification," in *From Data to Models and Back (DataMod2024)*, Springer International Publishing, 2024.

2. **K. Ye**, R. Metere, and P. Yadav, "User-Guided Verification of Security Protocols via Sound Animation," in *Software Engineering and Formal Methods*, Springer Nature Switzerland, Nov. 2024, pp. 33–51, ISBN: 9783031773822. DOI: 10.1007/978-3-031-77382-2_3.

3. M. Adam, **K. Ye**, D. A. Anisi, A. Cavalcanti, J. Woodcock, and R. Morris, "Probabilistic Modelling and Safety Assurance of an Agriculture Robot Providing Light-Treatment," in *2023 IEEE 19th International Conference on Automation Science and Engineering (CASE)*, ISSN: 2161-8089, Aug. 2023, pp. 1–7. DOI: 10.1109/CASE56687.2023.10260395. (visited on 10/13/2023).

4. **K. Ye**, S. Foster, and J. Woodcock, "Formally Verified Animation for RoboChart Using Interaction Trees," en, in *Formal Methods and Software Engineering*, A. Riesco and M. Zhang, Eds., ser. Lecture Notes in Computer Science, Cham: Springer International Publishing, 2022, pp. 404–420, ISBN: 978-3-031-17244-1. DOI: 10.1007/978-3-031-17244-1_24.

5. **K. Ye**, S. Foster, and J. Woodcock, "Automated Reasoning for Probabilistic Sequential Programs with Theorem Proving," en, in *Relational and Algebraic Methods in Computer Science*, U. Fahrenberg, M. Gehrke, L. Santocanale, and M. Winter, Eds., ser. Lecture Notes in Computer Science, Cham: Springer International Publishing, 2021, pp. 465–482, ISBN: 978-3-030-88701-8. DOI: 10.1007/978-3-030-88701-8_28.

6. J. Woodcock, A. Cavalcanti, S. Foster, A. Mota, and **K. Ye**, "Probabilistic Semantics for RoboChart," en, in *Unifying Theories of Programming*, P. Ribeiro and A. Sampaio, Eds., ser. Lecture Notes in Computer Science, Cham: Springer International Publishing, 2019, pp. 80–105, ISBN: 978-3-030-31038-7. DOI: 10.1007/978-3-030-31038-7_5.

7. S. Foster, **K. Ye**, A. Cavalcanti, and J. Woodcock, "Calculational Verification of Reactive Programs with Reactive Relations and Kleene Algebra," en, in *Relational and Algebraic Methods in Computer Science*, J. Desharnais, W. Guttmann, and S. Joosten, Eds., ser. Lecture Notes in Computer Science, Cham: Springer International Publishing, 2018, pp. 205–224, ISBN: 978-3-030-02149-8. DOI: 10.1007/978-3-030-02149-8_13.

Books and Chapters

1. J. Woodcock, S. Foster, A. Mota, and **K. Ye**, "RoboStar Technology: Modelling Uncertainty in RoboChart Using Probability," en, in *Software Engineering for Robotics*, A. Cavalcanti, B. Dongol, R. Hierons, J. Timmis, and J. Woodcock, Eds., Cham: Springer International Publishing, 2021, pp. 413–465, ISBN: 978-3-030-66494-7. DOI: 10.1007/978-3-030-66494-7_13. (visited on 10/13/2023).

2. **K. Ye**, S. Foster, and J. Woodcock, "Compositional Assume-Guarantee Reasoning of Control Law Diagrams Using UTP," en, in *From Astrophysics to Unconventional Computation: Essays Presented to Susan Stepney on the Occasion of her 60th Birthday*, ser. Emergence, Complexity and Computation, A. Adamatzky and V. Kendon, Eds., Cham: Springer International Publishing, 2020, pp. 215–254, ISBN: 978-3-030-15792-0. DOI: 10.1007/978-3-030-15792-0_10. (visited on 10/13/2023).

In Books

1. P. Ribeiro, **K. Ye**, F. Zeyda, and A. Miyazawa, "A tour through the programming choices: Semantics and applications," in *The Application of Formal Methods*. Springer Nature Switzerland, 2024, pp. 261–305, ISBN: 9783031671142. DOI: 10.1007/978-3-031-67114-2_11.

Preprints

1. **K. Ye** and J. Woodcock, *RoboCertProb: Property Specification for Probabilistic RoboChart Models*, 2024. arXiv: 2403.08136 [cs.LO].
2. **K. Ye**, F. Yan, and S. Gerasimou, *Quantitative Assurance and Synthesis of Controllers from Activity Diagrams*, 2024. arXiv: 2403.00169 [cs.LO].

PhD Thesis

1. **K. Ye**, "Model Checking of State-Rich Formalisms (By Linking to Combination of State-based Formalism and Process Algebra)," en, phd, University of York, Aug. 2016. URL: https://etheses.whiterose.ac.uk/15526/ (visited on 10/13/2023).

Conferences and Presentations

SEFM2024	Title: "User-Guided Verification of Security Protocols via Sound Animation". The slide is available at https://www-users.york.ac.uk/~ky582/SEFM2024/SEFM2024_presentation.pdf.
JWFS2024	Title: "A tour through the programming choices: semantics and applications" On the occasion of Jim Woodcock's Festschrift for his retirement from the University of York.
Lightning Talk 2024	Title: "Guarantee correctness and performance of probabilistic algorithms". The presentation video is available at https://www.youtube.com/watch?v=9GZMzrVsnxY on Youtube.
MODELS2022	Invited talk as a SoSym Journal-first award. Title: "Probabilistic modelling and verification using RoboChart and PRISM".
ICFEM2022	Title: "Formally Verified Animation for RoboChart Using Interaction Trees".
RAMICS2021	Title: "Automated Reasoning for Probabilistic Sequential Programs with Theorem Proving".
PoS2019	Pint of Science 2019. Title: "Engineering RoboGc Swarms".
Workshop	Workshop on Modelling, Verification, and Refinement of Evolving Cyber-Physical Systems, 2019. One-day "Isabelle/UTP Tutorial" to more than 20 students from Southwest University.

Teaching

2024 – 2025	Teaching assistant for the practical part of the course "Cryptography Theory and Practice" in the Department of Computer Science at the University of York.
2019 – 2020	Teaching assistant for the practical part of the course "Concurrent System Analysis & Verification (CSAV)" in the Department of Computer Science at the University of York.
2018 – 2019	Teaching assistant for the practical part of the course "Concurrent System Analysis & Verification (CSAV)" in the Department of Computer Science at the University of York.

Skills

Formal Languages	The Z notation, CSP, and Circus are the main languages used in my research. PRISM: a deep understanding of its semantics and language features for probabilistic model checking.
Semantic framework	Unifying Theories of Programming (UTP): correctness through refinement.
Theorem Proving	Isabelle/HOL: used in four research projects to create theories and prove algebraic laws for four languages.
Model checkers	PRISM and FDR: used for more than five years with a deep understanding of their language semantics (PRISM and CSP).
Probabilistic models	Markov models (DTMCs, MDPs, and CTMCs) and Bayesian Networks
Model-based techniques	Eclipse Modelling Framework (EMF), Eclipse Xtext and Sirius, and Eclipse Epsilon toolsets for model validation, transformation, and generation.
Functional languages	Haskell, the functional language in Isabelle/HOL, and Prolog.
Programming languages	C, C++, and Java
System Modelling	SysML: State machine diagrams and activity diagrams.