CONTACT INFORMATION
E-mail: mwicker@turing.ac.uk
Phone: [redacted]

RESEARCH INTERESTS

Machine Learning, Formal Verification, Adversarial Robustness, Algorithmic Fairness, Bayesian Methods, Trustworthy AI, Optimization, Probability Theory

CURRENT POSITION

Postdoctoral Research Associate May 2022 – present

The Alan Turing Institute, Artificial Intellegence & Finance and Economics
Project: Framework for responsible adoption of AI in the financial services industry
Supervisor: Adrian Weller

RESEARCH EXPERIENCE

Postdoctoral Research Associate Oct 2021 – May 2022

University of Oxford, Department of Computer Science, Oxford, UK
Project: FUN2MODEL, with a focus on guarantees for neural networks
Supervisor: Marta Kwiatkowska

Doctor of Philosophy (PhD/DPhil) Oct 2018 – Oct 2021

University of Oxford, Department of Computer Science, Oxford, UK
Submitted: October 2021 ***Passed Viva:*** November 2021
Thesis Project: Adversarial Robustness of Bayesian Neural Networks
Supervisor: Marta Kwiatkowska

Research Cluster Administrator Jan 2020 – present

Responsible for updating and maintaining group server cluster including on boarding new users, and purchasing new equipment.

Research Assistant May 2018 – Oct 2018

Moffitt Cancer Center, Dept. of Integrated Mathematical Oncology
Project: Deep Learning of Tumor-Treatment Dynamics and Control;
Supervisor: Alexander Anderson

Research Assistant Mar 2016 – May 2018

University of Oxford, Department of Computer Science, Oxford, UK
Project: Neural Network Falsification and Verification
Supervisor: Marta Kwiatkowska

Project: Modeling Oncological Cooperation and Evolutionary Dynamics
Supervisor: Pete Jeavons, Artem Kaznatcheev

Project: Practical Verification of Programs Written in High Level Languages
Supervisor: Marta Kwiatkowska, Xiaowei Huang

Research Assistant Aug 2016 – May 2018

University of Georgia, Department of Computer Science, Athens, GA, USA
Project: Dynamic Programming Algorithms for Ab Initio RNA Modeling
Supervisor: Liming Cai

Project: Graph Embedding Algorithms for RNA Structure Analysis
Supervisor: Liming Cai

Committees and Reviewing

Conference Reviewing: NeurIPS (2019 - 2022), ICLR (2019 - 2022), ICML (2021, 2022), AAAI (2020, 2021), IJCAI (2022), AISTATS (2022), CVPR (2019), HSCC (2021, 2022)
Journal of Machine Learning Research Reviewer
Computer Aided Verification Journal Reviewer
Transactions on Machine Learning Research Reviewer
OxCSC 2019 Oxford Computer Science Conference Programming Comittee
CVPR 2019 Adversarial Machine Learning Programming Committee
CVPR 2019 Security and Privacy Programming Committee
NeurIPS 2018 Security and Privacy Reviewer

TEACHING EXPERIENCE

Tutor (University of Oxford) October 2020 - Present

Advanced Machine Learning (Practicals/Masters Level)	2022
Computer Aided Formal Verification (Masters Level)	2021
Computer Security (Masters Level)	2021
Computer Security (Undergraduate Level)	2021
Knowledge Reasoning and Representation (Marker)	2020

Mentoring and Short Courses

An Introduction to Bayesian Deep Learning - Guest Lecture + Course Assignment, Royal Holloway, University of London, 2022

Research Mentor - Mentored an undergraduate student from University of Georgia. Taught introductory machine learning and research methods. October 2021 - February 2022

Mentored for Junior Research Project - Co-mentored an undergraduate student from Princeton University towards the completion of a research report on adversarial robustness of Bayesian Neural Networks. Resulted in paper [P10]. October 2020 - January 2021

An Introduction to Modern Machine Learning Methods - Invited Lecture, University of Southern Florida, 2018

Reading Course on Safety of Machine Learning - Organized lecture series for the QAV group.

An Introduction to Bayesian Learning - Designed and Delivered course work to students aged 13-14 on Bayesian learning. Due to positive student response, I have been invited to run the course again. June, 2022

Admissions Assistant - New College, University of Oxford, 2018

EDUCATION

Doctor of Philosophy Oct 2018 – Oct 2021

University of Oxford, Department of Computer Science, Oxford, UK
Thesis Project: Adversarial Robustness of Bayesian Neural Networks
Supervisor: Marta Kwiatkowska

Bachelor's Degree May 2018

University of Georgia, Franklin College of Arts and Sciences, Athens, GA, USA
Major: Computer Science
GPA: 3.89/4.00 *Major GPA:* 4.00/4.00

University of Oxford (Visiting Student), Keble College, Oxford, UK
Major: Computer Science; *GPA:* 3.93/4.00

Selected Papers

[P1] M. Wicker, X. Huang, M. Kwiatkowska. *Feature-Guided Black-Box Safety Testing of Deep Neural Networks.* In Tools and Algorithms for the Construction and Analysis of Systems (TACAS) 2018. https://arxiv.org/abs/1710.07859

[P2] M. Wu, M. Wicker, W. Ruan, X. Huang, M. Kwiatkowska. *A Game-Based Approximate Verification of Deep Neural Networks with Provable Guarantees.* In Journal of Theoretical Computer Science. https://arxiv.org/abs/1807.03571

[P3] M. Wicker, M. Kwiatkowska. *Robustness of 3D Deep Learning in an Adversarial Setting.* In IEEE Computer Vision and Pattern Recognition (CVPR) 2019. https://arxiv.org/pdf/1904.00923.pdf

[P4] L. Cardelli, M. Kwiatkowska, L. Laurenti, N. Paoletti, A. Patane*, M. Wicker*. *Statistical Guarantees for the Robustness of Bayesian Neural Networks.* International Joint Conference on Artificial Intelligence (IJCAI) 2019. https://arxiv.org/pdf/1903.01980.pdf

[P5] M. Wicker*, A. Patane*, L. Laurenti*, M. Kwiatkowska. *Probablistic Safety for Bayesian Neural Networks.* Uncertainty and Artificial Intellegence (UAI) 2020. https://arxiv.org/pdf/2004.10281.pdf

[P6] M. Wicker*, L. Laurenti*, A. Patane, N. Paoletti, A. Abate, M. Kwiatkowska *Certification of Iterative Predictions in Bayesian Neural Networks.* UAI 2021. https://arxiv.org/pdf/2004.10281.pdf

[P7] G. Carbone*, M. Wicker*, L. Laurenti, A. Patane, L. Bortolussi, G. Sanguinetti *Robustness of Bayesian Neural Networks to Gradient-Based Attacks.* Conference on Neural Information Processing Systems (NeurIPS) 2020. https://arxiv.org/pdf/2002.04359.pdf

[P8] R. Michelmore*, M. Wicker*, L. Laurenti, L. Cardelli, Y. Gal, M. Kwiatkowska *Uncertainty Quantification with Statistical Guarantees in End-to-End Autonomous Driving Control.* International Conference on Robotics and Automation (ICRA) 2020. https://arxiv.org/pdf/1909.09884.pdf

[P9] M. Wicker*, L. Laurenti*, A. Patane*, Z. Chen, Z. Zhang, M. Kwiatkowska *Bayesian Inference with Certifiable Adversarial Robustness.* 24th International Conference on Artificial Intelligence and Statistics (AISTATS). http://proceedings.mlr.press/v130/wicker21a.html

[P10] E. Benussi, A. Patane, M. Wicker, L. Laurenti, M. Kwiatkowska *Individual Fairness Guarantees for Neural Networks.* International Joint Conferences on Artificial Intelligence (IJCAI) 2022. https://arxiv.org/abs/2205.05763

[P11] B. Wang, M. Wicker, M. Kwiatkowska *Causal Structure Learning with Tractable Uncertainty.* International Conference on Machine Learning, 2022. https://arxiv.org/abs/2204.14170

[P12] M. Yuan, M. Wicker, L. Laurenti *Gradient-Free Adversarial Attacks for Bayesian Neural Networks.* Advances in Approximate Bayesian Inference (AABI). https://arxiv.org/pdf/2012.12640.pdf

[P13] M. Strobl, M. Wicker, V. Adhikarla, A. Shockey, E. Lakatos, P. Pooladvand, R. Schenk, L. Saputro, C. Gatenbee, M. Koppens, S. García, R. Wenham, M. Damaghi, J. Gallaher. *Connecting the Microenvironmental Niche to Treatment Response in Ovarian Cancer.* https://www.biorxiv.org/content/10.1101/452052v1

[T1] M. Wicker, *Adversarial Robustness of Bayesian Neural Networks.* PhD Thesis. University of Oxford. https://ora.ox.ac.uk/objects/uuid:9086791d-4b4d-41ca-9835-7a504cd6c35c

SELECTED PAPERS (CONT.)

[**P14**] M. Wicker, L. Laurenti, A. Patane, M. Kwiatkowska *Probabilistic Verification of Bayesian Neural Networks.* to be submitted to IEEE Transactions on Neural Networks and Learning Systems.

[**P15**] M. Wicker, L. Laurenti, N. Paoletti, M. Kwiatkowska, A. Abate *Synthesizing Certifiable Control Strategies for Bayesian Neural Network.* Minor corrections needed to appear in Artificial Intelligence Journal.

[**P16**] L. Bortolussi, G. Carbone, L. Laurenti, A. Patane, G. Sanguinetti, M. Wicker *On the Robustness of Bayesian Neural Networks to Adversarial Attacks.* Submitted to Journal of Machine Learning Research.
https://arxiv.org/pdf/2207.06154.pdf

[**P17**] M. Wicker, J. Heo, L. Costabello, A. Weller, *Robust Explanation Constraints for Neural Networks.* Accepted to ICLR 2023, *https://arxiv.org/pdf/2212.08507.pdf*

[**P18**] E. LaMalfa, M. Wicker, M. Kwiatkowska, *Emergent Linguistic Structures in Neural Networks are Fragile.* Pre-print. https://arxiv.org/pdf/2210.17406.pdf

[**P19**] V. Piratla, J. Heo, M. Wicker, A. Weller *Robust Learning from Explanations.* Submitted to ICML 2023.

[**P20**] M. Wicker, V. Piratla, U. Bhatt, A. Weller *Certified Individual Fairness Adaptation for Neural Networks.* To be submitted to UAI 2023.

[**P21**] M. Wicker, L. Yingzhen, *Ensembles with Certified Uncertainty.* To be submitted to UAI 2023.

AWARDS

University of Oxford - Google DeepMind Scholar 2019 – 2021
Scholarship covering entire DPhil course and living stipend at the University of Oxford.

University of Georgia Classics Scholar 2014 – 2018
Scholarship waiving out-of-state tuition fees based on high standardized test scores.

Best Paper Award 2022
Received Best Paper Award at ICML Workshop on Tractable Probabilistic Methods

Integrated Mathematical Oncology Workshop Winner 2018
Worked on an interdisciplinary team in a hackathon-style competition.
Won competition for $50,000 in grant money for project studying thyroid cancers.

Integrated Mathematical Oncology Travel Grant 2017, 2018
Awarded full travel and accommodations to attend the 7th Integrated Mathematical Oncology workshop in Tampa, Florida.

CURO Research Assistantship Grant 2016 – 2017
Awarded to undergraduate students pursuing research. Awarded repeatedly.

CURO Conference Travel Fellowship 2017
Travel stipend to attend and present at ISMB/ECCB in Prague, Czech Rebublic.

Learning Technologies Grant 2016
Research grant to explore use of hardware in large lecture classes. Later used to analyze sociological effect of incorporating new technology into the classroom.

Randall H. Pettus Who's Who Recipient 2016
Nominated by professor and selected by department heads for outstanding departmental contributions.

AWARDS (CONT.)

Oxford Union Floor Speech Prize 2016
Recognized for best floor speech at the Oxford Union Debate on cyber security.

Select Honor Societies
Dean's List, 2014 – 2017: Achieving greater than 3.65/4.00 GPA
President's List, 2018: Achieving 4.00/4.00 GPA
Phi Beta Kappa, 2018: Outstanding member of top 10% of UGA BS graduates.
Phi Kappa Phi, 2018: Oustanding member of top 15% of UGA graduates.

TALKS AND PRESENTATIONS

[**T1**] *Learning Models with Provably Robust Explanations,* Invited Talk, FAIR Symposium. 2023.

[**T2**] *Towards Provably Trustworthy ML in Finance,* Accenture-Turing Joint Strategy Meeting. 2023.

[**T3**] *Provable Robustness in Bayesian Deep Learning,* Invited Talk, Imperial College. 2022.

[**T4**] *The Benefits of Being Bayesian (in Deep Learning),* Invited Talk, Waymo Research. 2022.

[**T5**] *Certification of iterative predictions in Bayesian neural networks,* UAI recorded presentation, Virtual. 2021.

[**T6**] *Bayesian Inference with Certifiable Adversarial Robustness,* AISTATS spotlight talk, Virtual. 2021.

[**T7**] *Probabilistic Safety for Bayesian Neural Networks,* UAI recorded presentation, Virtual. 2020.

[**T8**] *Statistical Robustness Guarantees for Bayesian Neural Networks,* Statistics and Computation workshop, Alan Turing Institute. 2020.

[**T9**] *An Introduction to Modern Machine Learning Methods,* Invited Lecture, University of Southern Florida, 2018.

[**T10**] *Deep Regression for Learning Tumor-Treatment Dynamics,* Research talk at Department of Integrated Mathematical Oncology, 2018.

[**T11**] M. Strobl, M. Wicker, R. Wenham, M. Damaghi, J. Gallaher. *The Role of Niche Heterogeneity in Initiation and Metastasis of Ovarian Cancer,* 7th Integrated Mathematical Oncology workshop presentation. 2017.

[**T12**] *Evolutionary Dynamics of Growth Factor Production,* Moffitt Department of Oncology Research. Workshop Poster, 2017.

[**T13**] *Modeling the dynamics of oncological growth factor production* Moffitt Department of Oncology Research. Invited Talk, 2017.

[**T14**] *Automated Realization of RNA Structure from Interaction Topology.* Poster Presentation at ISMB/ECCB 2017.

[**T15**] *Evaluating the Robustness of Neural Networks.* Talk at meeting of the University of Oxford Verification Group, 2017.

[**T16**] S. Clouser, M. Wicker, J. Coverdill, B. Barnes. *Attendance Matters. Using Brightspace API for Attendance in Large Classes* Talk at Desire2Learn FUSION Conference 2017.

[**T17**] *Graph Theoretic Approach for RNA Visualization.* Talk at UGA CURO Symposium, 2017.

[**T18**] *Visualization of Higher Order Relations in Biological Graphs.* Poster Presentation UGA Graduate Research Symposium, 2017.