Robust Decision Pipelines: Opportunities and Challenges for AI in Business Process Modelling[⋆]

Marta Kwiatkowska[1][0000−0001−9022−7599]

Department of Computer Science, University of Oxford, UK
marta.kwiatkowska@cs.ox.ac.uk

Keywords: Modelling and verification · Adversarial robustness · Optimality guarantees.

1 Extended Abstract

Traditional business process modelling techniques, which leverage handcrafted pipelines and expert knowledge, are being revolutionised by artificial intelligence (AI). Deep learning (DL), in particular, has been successfully employed in process mining and discovery to build predictive process models from event logs [1], and reinforcement learning (RL) can be utilised for policy synthesis. Data-driven decision pipelines are now commonly deployed in application domains such as financial services, and rigorous modelling of the associated processes can aid in their stress testing, optimisation and 'what if' analysis.

However, a known concern about DL is that it lacks robustness; more specifically, DL systems such as neural networks are susceptible to so called adversarial attacks, i.e., minor modifications to inputs, often imperceptible, which can catastrophically change the decision of the network. Before they can be deployed within decision pipelines, DL components require certifiable guarantees not just for accuracy and performance, but also properties such as safety and robustness [2].

Fortunately, much progress has been made in formal modelling and verification techniques, especially model checking, with which rigorous models of software systems can be built and automatically checked against specifications expressed in temporal logic [3]. Building on existing verification technologies, a fast growing research effort is tackling the problem of computing robustness guarantees for deep learning; examples include search-based safety verification using SMT (Satisfiability Modulo Theory) [2] for DL, guaranteed robust explanations for DL [4], provable robustness to causal interventions for DL decisions [6], and optimality guarantees for RL policies from temporal logic specifications [5].

[⋆] Supported by the EPSRC Prosperity Partnership FAIR (grant number EP/V056883/1). MK receives funding from the ERC under the European Union's Horizon 2020 research and innovation programme (FUN2MODEL, grant agreement No. 834115).

However, while data-rich scenarios and deep learning enable ease of automation for business processes, they also present significant new challenges due to their complexity, as well as their black-box and adaptive nature. Achieving robust decision pipelines will require concerted effort to develop integrated methods for certifiable training, robust explainability, certification guarantees, robustness to distribution shift and interventions, optimal policy synthesis and real-time monitoring.

References

1. Evermann, J., Rehse, J.R., Fettke, P.: Predicting Process Behaviour using Deep Learning. Decision Support Systems **100**, 129–140 (2016)
2. Huang, X., Kwiatkowska, M., Wang, S., Wu, M.: Safety Verification of Deep Neural Networks. In: Proc., Computer Aided Verification CAV 2017. Springer (2017)
3. Kwiatkowska, M., Norman, G., Parker, D.: PRISM 4.0: Verification of probabilistic real-time systems. In: Proc. 23rd International Conference on Computer Aided Verification (CAV'11). pp. 585–591. Springer (2011)
4. La Malfa, E., Zbrzezny, A., Michelmore, R., Paoletti, N., Kwiatkowska, M.: On guaranteed optimal robust explanations for NLP models. In: Proc. International Joint Conference on Artificial Intelligence (IJCAI-21) (2021)
5. Shao, D., Kwiatkowska, M.: Sample Efficient Model-free Reinforcement Learning from LTL Specifications with Optimality Guarantees. In: Proc., International Joint Conference on Artificial Intelligence (IJCAI) (2023)
6. Wang, B., Lyle, C., Kwiatkowska, M.: Provable guarantees on the robustness of decision rules to causal interventions. In: Proc. International Joint Conference on Artificial Intelligence (IJCAI-21) (2021)