Scalable DNN Verification using Constraint Solving

Speaker: Prof. Thanhvu Nguyen
Department of Computer Science
George Mason University
Friday, September 23, 2022
1-2PM, NVC 214

Abstract

Deep Neural Networks (DNNs) have emerged as an effective approach to tackling real-world problems. However, just like traditional software, DNNs can have “bugs” and be attacked. This naturally raises the question of how DNNs should be tested, validated, and ultimately verified to meet the requirements of relevant robustness and safety standards. To address this question, researchers have developed powerful formal methods and tools to verify DNNs. However, despite many recent advances, these approaches and tools still have challenges in achieving good precision and scalability. In this talk, we will present our recent development on using constraint solving for scalable DNN reasoning. The insight of the work is integrating the successful conflict clause learning technique in SAT solving with fast abstractions in DNN verification to obtain scalable and precise DNN verification. Preliminary results show that our prototype implementation is several magnitudes faster than popular and state-of-the-art constraint solving-based DNN verification tools.

Biography

ThanhVu Nguyen is an assistant professor in the Department of Computer Science at George Mason University. Prior to joining GMU, he was at the University of Nebraska-Lincoln. He received his Ph.D. in Computer Science from the University of New Mexico-Albuquerque and completed a two-year postdoc at the University of Maryland-College Park. His research is in the intersection of Software Engineering and Programming Languages. In particular, he focuses on improving software quality through static verification and reasoning, dynamic invariant inference, automatic program repair, and highly-configurable systems analysis. He is a recipient of the NSF CISE Career Research Initiation Initiative (CRII) Award, a 10-year Most Influential Paper award (at ICSE 2019), and a 10-year Impact Paper Award (at GECCO 2019).