Testing Deep Neural Networks (Keynote)

Mary Lou Soffa
University of Virginia
USA
soffa@virginia.edu

Abstract

The reliability of software that has a Deep Neural Network (DNN) as a component is urgently important today given the increasing number of critical applications being deployed with DNNs. The need for reliability raises a need for rigorous testing of the safety and trustworthiness of these systems. In the last few years, there have been a number of research efforts focused on testing DNNs. However, the test generation techniques proposed so far lack a check to determine whether the test inputs they are generating are valid, and thus invalid inputs are produced. To illustrate this situation, we explored three recent DNN testing techniques. Using deep generative model based input validation, we show that all the three techniques generate significant number of invalid test inputs. We further analyzed the test coverage achieved by the test inputs generated by the DNN testing techniques and showed how invalid test inputs can falsely inflate test coverage metrics. To overcome the inclusion of invalid inputs in testing, we propose a technique to incorporate the valid input space of the DNN model under test in the test generation process. Our technique uses a deep generative model-based algorithm to generate only valid inputs. Results of our empirical studies show that our technique is effective in eliminating invalid tests and boosting the number of valid test inputs generated.

CCS Concepts: • **Software and its engineering → Software maintenance tools**.

Keywords: Deep Neural Networks; Testing of Deep Neural Networks; Invalid Input; Variational Autoencoder

ACM Reference Format:
Mary Lou Soffa. 2020. Testing Deep Neural Networks (Keynote). In *Companion Proceedings of the 2020 ACM SIGPLAN International Conference on Systems, Programming, Languages, and Applications: Software for Humanity (SPLASH Companion '20), November 15–20, 2020, Virtual, USA.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3426430.3434071

Biography

Mary Lou Ehnot Soffa is the Owen R. Cheatham Professor of Sciences at the Computer Science Department at the University of Virginia. From 2004 to 2012, she served as the Department Chair at UVA. From 1977 to 2004, she was a Professor of Computer Science at the University of Pittsburgh and also served as the Dean of Graduate Studies in the College of Arts and Sciences from 1991 to 1996. Her research interests include optimizing compilers, virtual execution environments, software testing, program analysis, software security, and software systems for multi-core architectures. She has published over 175 articles and has directed 32 Ph.D. students to completion, half of whom are women. Mary Lou is both an IEEE Fellow and an ACM Fellow. She received the Anita Borg Technical Leadership Award, the Ken Kennedy Award and the Computing Research Association (CRA) Nico Habermann Award.

SPLASH Companion '20, November 15–20, 2020, Virtual, USA

ACM ISBN 978-1-4503-8179-6/20/11.
https://doi.org/10.1145/3426430.3434071