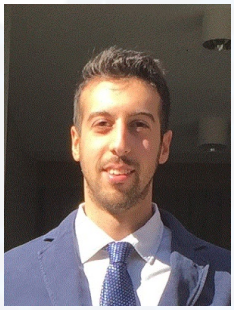
Resilient and Energy-Efficient Deep Learning with Capsule Networks and Spiking Neural Networks



Politecnico di Torino - Aula 2T
18 February 2020 -11.00 AM

Mr. Alberto Marchisio,
TU Wien, Austria

TU WIEN TECHNISCHE UNIVERSITÄT WIEN

ABSTRACT

Deep Neural Networks (DNNs) have shown high level of accuracy in several tasks, therefore they are widely used in many systems and platforms. Recent researches have demonstrated, however, that such networks are vulnerable to malicious attacks, who are able to fool the network. These security issues are extremely challenging for safety-critical applications, where such errors are not tolerable.

Moreover, DNNs are high-resource demanding, because of their computational complexity (matrix multiplications) and memory accesses. From the software perspective, several techniques have been explored for reducing the complexity of training and inference, e.g., approximations, pruning, quantization. From the hardware perspective, specialized accelerators are required to achieve high performance training (in GPU/datacenters) and at the edge, in order to meet timing constraints (latency) in a limited power budget. Efficiently mapping DNN workloads into the accelerator is also a challenging task.

Recently, a specialized neural network architecture composed of capsules, called Capsule Networks (CapsNets), has been demonstrated to overcome standard DNNs, because the feature representations stored inside the capsules are in vector/matrix form, compared to the neurons in scalar form. However, its complexity makes a challenging problem to keep high performance and energy efficiency. Therefore, specialized hardware accelerators for CapsNets are required to achieve these goals. This requires investigation of energy-efficient compute fabrics, specialized memory hierarchy, and appropriate data flow mapping techniques. Besides DNNs, Spiking Neural Networks (SNNs), i.e., networks whose information is propagated through spikes, have demonstrated to be more powerful and energy efficient, compared to their DNN counterparts. Spiking neurons are similar to / inspired by the biological neurons, but still there is a huge gap in terms of energy efficiency between SNNs and the brain. Hence, specialized hardware accelerators for SNNs, e.g., neuromorphic architectures, need to be analyzed/improved. On another note, considering the importance of secure systems and recent investigations in adversarial machine learning, CapsNets and SNNs will also require an extensive analysis of security vulnerabilities and defenses, before they could be deployed in the use-cases from real world systems. Due to a different processing flow, they exhibit different properties compared to traditional DNNs. Therefore, their robustness against adversarial attacks and soft errors may change significantly, and would therefore, require a different set of studies for analysis and design of robustness techniques for them.

BIO

Mr. Alberto Marchisio received his B.Sc. degree in Electronic Engineering from Politecnico di Torino, Turin, Italy, in October 2015. He received his M.Sc. degree in Electronic Engineering (Electronic Systems) from Politecnico di Torino, Turin, Italy, in April 2018. Currently, he is Ph.D. Student at Computer Architecture and Robust Energy-Efficient Technologies (CARE-Tech.), Embedded Computing Systems, Department of Informatics, Institute of Computer Engineering, Technische Universität Wien (TU Wien), Vienna, Austria, under the supervision of Prof. Dr. Muhammad Shafique. He is also a student IEEE member. His main research interests include VLSI architecture design, machine learning, brain-inspired computing, emerging computing technologies, robust and approximate computing. He received the honorable mention at the Italian National Finals of Maths Olympic Games in 2012. He also received the Richard Newton Young Fellow Award in 2019.