Washington University in St. Louis
Office of Technology Management

ERROR CORRECTING CODES FOR ROBUST, SECURE DEEP NEURAL NETWORKS

Raviv, Netanel

Maland, Brett

T-019252

Technology Description

Researchers in Prof. Netanel Raviv's laboratory have developed a provable error correcting code (ECC) system that could guarantee deep neural networks (DNN) are resilient to noise for robust, secure and private neural computation. This technology could be deployed in neural network hardware, particularly for critical applications such as autonomous driving.

Currently, neural computation is highly sensitive to both malicious and random noise, making DNNs less secure and difficult to implement in hardware. Conventional techniques to solve this data corruption problem require retraining which can't provably guarantee resilience to noise and involves intractable optimization problems. As an alternative, simple ECCs offer a fundamentally new method for combatting noise by inserting redundancy through extra bits of input or added neurons. This system uses a novel geometric approach which could guarantee that resulting computations are provably true even in the presence of malicious entities. This technology could potentially extend the success of ECCs from traditional computing to the realm of neural networks, guaranteeing successful computation, security, privacy and robust classification with a very low computational overhead.

Example of ECC for DNN *– Stickers on a stop sign create noise. Conventional trained models misidentify this as a speed limit sign while ECC creates redundancy that guarantees correct classification.*

Stage of Research

The inventors demonstrated proof-of-concept of coded neural computation using a parity code that guaranteed successful classification under noise for a large family of deep neural networks.

Publications: Raviv, N., Jain, S., Upadhyaya, P., & Bruck, J. (2020). CodNN--Robust Neural Networks From Coded Classification. arXiv preprint arXiv:2004.10700.

Applications

- **Neural network hardware** – ECC integrated on-chip for robust deep neural networks with end user applications

such as:
- autonomous vehicles
- phones
- sensors
- healthcare devices

Key Advantages

- **Highly resilient to both malicious and random noise:**
  - mathematically rigorous guarantees that are provable, not probabilistic
  - no retraining needed
- **Secure, private computation -** no information about the input can be inferred by a person holding the network
- **Low computational overhead**

Patents: Application filed

Related Web Links: Raviv Profile