Synchronous Neural Networks for Cyber-Physical Systems

Notes:

* CPS must be “safe”, so having “safe” in title may not be necessary.
* ANNs must be mentioned.
* Synchronous probably does not have to be mentioned.
* CPS should be mentioned; they are a core component of this field of research.

Abstract:

*Cyber-physical systems (CPS), such as autonomous vehicles or smart power grids, use interactive machine learning modules for decision making. Current design approaches use multiple machine learning modules, often using Artificial Neural Networks (ANNs), to achieve the desired functionality. Current approaches to verification and validation of these ANNs are generally either very difficult, time consuming and/or not fully reliable. A key feature missing is related to the use of NNs in real-time systems, which demand the capability of worst case analysis.*

*A new approach to verifiable ANNs is proposed using the synchronous paradigm to introduce Synchronous Neural Networks (SNNs). Logical time is allocated to the operations of the SNNs, providing sound compositional primitives. This enables the composition of interacting ANNs to ensure causality and determinism.*

*In this thesis we introduce SNNs as a new approach to the safe use of ANNs in CPS. We mathematically verify these SNNs using formal methods, and when embedded on time predictable platforms, static analysis of these SNNs is enabled. Additionally, we propose the combination of SNNs and other synchronous functional components, notably Runtime Enforcement (RE), by formally defining Meta Neural Networks (MNNs). These synchronous MNNs allow for the creation of causal, deterministic, predictable controllers for CPS.*

*ANNs for this thesis were implemented in Esterel for the design of synchronous, predictable systems. We demonstrate the efficacy of our approach by developing CPS with MNN controllers; ranging from MNNs with 5 neurons to MNNs with 10,000+ neurons. This thesis also introduces a compiler that converts ANNs created and trained using Keras to the predictable MNNs previously introduced.*

Notes:

* Wanted to mention CPS.
* Introduced the overall concept of SNNs first, and what they enable.
* Then mentioned the combination of synchronous components, i.e. MNNs.
* Mentioned Esterel and MNN2C.
* Mentioned what the benchmarks will be.

The abstract is reasonable but incomplete. You have to highlight all contributions

1. SNNs that provide a synchronous semantics to NNs. This enables periodic real-time operation and facilitates static timing analysis of individual NNs.
2. We propose meta neural networks (MNNs) as a framework for systematic composition of multiple NNs. This enables compositional system design using multiple NNs.
3. We combine NNs with run-time enforcers, which enforce a set of desired policies by transforming the inputs and outputs suitably. These enforced SNNs (ESNNs) are shown to be able to effectively deal with mis-predictions so as to avoid safety violations.
4. Finally, we propose a tool that extends Keras to give it a MNN description capability. We then automatically generate C code, which are shown to perform even better than our earlier MNN implementations using Esterel.