Overview of Projects

[Submitting to AAAI 2024] Efficient and Principled Algorithms for Neural Active Learning by Yikun Ban*, **Ishika Agarwal***, Hanghang Tong and Jingrui He

We study both stream-based and pool-based active learning with neural network approximations. A recent line of works proposed bandit-based approaches that transform active learning into a bandit problem, achieving both theoretical and empirical success. However, these type of methods incur the additional computational cost that is scaled by the number of classes K due to this transformation. In contrast, the classic active learning algorithms will not be burdened by the extra computational cost, but they lack the principled exploration and provable performance guarantee compared to bandit-based methods. Therefore, this paper seeks to answer the question: "How can we remove this incurred computation burden while still enjoying the principled exploration and provable performance guarantee for active learning?" We propose two algorithms based on the newly designed exploitation and exploration neural networks for stream-based and pool-based active learning respectively. Then, we provide the theoretical performance guarantee for these two algorithms in the non-parametric setting by removing the dependency on function class radius.In the end, we use extensive experiments to evaluate the proposed algorithms, which consistently outperform state-of-the-art baselines. (* Equal Contribution)

Active Graph Anomaly Detection using Bi-Level Optimization by **Ishika Agarwal**, Qinghai Zhou and Hanghang Tong

We are exploring how to find anomalies in graph data using active learning, generative models and bi-level optimization. Given a graph with nodes, node attributes, edges and an oracle, we will try to learn a strong enough autoencoder that can learn the distinction between anomalous and benign nodes. Similar to real life, we do not have labels, but we have a human annotator who can make an educated guess for the label. From the human annotator, we will receive the label and their confidence (percentage) – we claim that we can use the soft label to learn highly accurate hard labels.

Generative Transformers for Diverse Text Generation by **Ishika Agarwal**, Priyanka Kargupta, Bowen Jin, and Akul Joshi

Diverse text generation is an important and challenging task. Existing methods mainly adopt a discriminative model, with the underlying assumption that the input text-to-output text projection is a one-one mapping. However, this is not true in the real world, since given one single input text, there can be multiple ground truth output text candidates. For example, in the commonsense generation, given a list of knowledge entities, there should be more than one way to use them to come up with a sentence. This motivates us to capture the underlying text semantics distribution with generative models (e.g., VAE and diffusion models). On the other hand, Transformer architecture has been demonstrated to be effective in text semantics capturing. Then the problem comes to how to effectively combine the Transformer architecture with the generative models. Our project aims to combine the best of both worlds by introducing VAE & Diffusion model into transformers. Specifically, we want to apply them to two downstream tasks: common sense generation and question generation. We include results, and some future work to further this project.

[Submitted to AI-ML Systems 2023] QuickAns: A Virtual Teaching Assistant by **Ishika Agarwal**, Shradha Sehgal, Varun Goyal, and Prathamesh Sonawane

QuickAns is a virtual teaching assistant designed to assist course staff who use Campuswire as their Q&A platform. It reads Campuswire posts from digest emails and sends a potential answer to the course staff. At this stage, the course staff can review the answer for any logistical issues and answer a student's question in a matter of minutes.

[Published to SafeAI 2021 in AAAI] HiSaRL: A Hierarchical Framework for Safe Reinforcement Learning by Zikang Xiong, **Ishika Agarwal**, and Suresh Jagannathan

We propose a two-level hierarchical framework for safe reinforcement learning in a complex environment. The high-level part is an adaptive planner, which aims at learning and generating safe and efficient paths for tasks with imperfect map information. The lower-level part contains a learning-based controller and its corresponding neural Lyapunov function, which characterizes the controller's stability property. This learned neural Lyapunov function serves two purposes. First, it will be part of the high-level heuristic for our planning algorithm. Second, it acts as a part of a runtime shield to guard the safety of the whole system. We use a robot navigation example to demonstrate that our framework can operate efficiently and safely in complex environments, even under adversarial attacks.