Ishika Agarwal https://agarwalishika.github.io/ ishikaa2@illinois.edu

Statement of Purpose

of Ishika Agarwal (CS PhD applicant for Fall 2024)

Model developers collect as much data as possible and train a model to extract the meaning. The model's quality heavily depends on the data's quality. However, improving the quality and annotating voluminous data is laborious and expensive. My research interests lie in improving model quality while reducing costs by filtering for highly informative data from noisy data. One such strategy is active learning.

Active learning requires careful experimentation and design. There are three central questions: Which data points are most informative? How do we annotate the selected data points? Once we get the labels, how do we maximize the information gained from the labeled data?

Following are my major research projects over the past three years, where I learned about this area and cultivated my interests.

Hierarchical Safe Reinforcement Learning. I developed an interest in research during my undergrad at Purdue. During my junior year, I worked with Professor Suresh Jagannathan and his team for 3 semesters to develop a new algorithm to make reinforcement learning model training safe and efficient Xiong, Agarwal, and Jagannathan (2022). The solution has two levels: a high-level planner that creates a plan for an agent to complete the desired task, and a low-level controller that executes the plan. The controller might deviate from the plan, and therefore, a Lyapunov neural network is employed to guarantee that an agent does not encounter an unsafe state.

In this project, I wrote the code for the high-level planner, tuned the hyperparameters, and simulated experiments. Our paper was accepted at SafeAI, a workshop in AAAI. I also presented this work at the Purdue University Fall Research Expo.

I am currently pursuing a research-oriented Master's degree at UIUC. I am fortunate to be offered an RA-ship in Professor Hanghang Tong's IDEA lab.

Performative Neural Bandits for k-classification. I worked with Professor Tong and his team to develop a multi-armed bandit training algorithm that is not only efficient resource- and label-wise, but also combines the benefits of exploration and exploitation. In this project, we use the original input data (instead of transforming it into a long vector [1]), and a simple neural network of 2 layers. This is a label-efficient method because we employ active learning. We provide two methods for stream-based and pool-based active learning. For some datasets, our algorithm cuts prediction time of the model to 1/10th**** of the baseline while still improving accuracy by 10-12%.

I implemented all the algorithms, experimented/researched different strategies to improve our algorithm, researched the baselines, performed all the experiments, and tuned hyperparameters.

We experienced a few resubmissions of this paper (NeurIPS 2023). By improving this work progressively, I have learned not to be discouraged by rejections. Working with reviewers has helped me understand the rebuttal process and has improved my writing skills. We are submitting it to ICLR 2024, where I am a joint author on the paper.

Concept-Shift Agnostic Graph Anomaly Detection. I am leading another project on graph anomaly detection under Professor Hanghang Tong. We are researching a semi-self-supervised algorithm that can learn dense representations of input data. From the dense representations, we can train a lightweight classifier that can separate the anomalies from the benign points.

Realistically, obtaining hard labels can be difficult. We aim to account for label confidence by using soft labels. From the soft labels, we aim to augment the data by using mix-up as it can help make the distribution robust to concept-shift data points. Finally, we model this as a bi-level optimization problem in which each level learns one of the two components of the algorithm. This can alleviate the heavy cost of retraining by only having to retrain the lightweight classifier.

[1] A k-dimensional vector would transform to a k-dimensional vector where k is the number of classes. The label is also transformed into a vector of zeros and the label value is determined by a '1' in the index of the label.

I am planning to orient my Master's thesis around this project and extend it to a conference paper by Spring 2024. Additionally, I am submitting a tutorial on closed-loop graph anomaly detection to SDM 2024 with Dr. Qinghai Zhou, a recent graduate from our lab.

Industry Experience. I had the opportunity to contrast my research experience with industrial experience. I interned at Apple and Cisco, and between BS and MS, I worked full-time at Cisco as a Software Engineer for six months. While I learned a lot in the industry, I found that I thrive more in the open-ended environment of research. I love exploring fundamental questions and advancing the state of knowledge in my field, which I can do more freely in academia. I also enjoy all aspects of academic life, such as writing, reviewing, presenting, teaching, and mentoring.

At the University of Washington I plan to continue my interests in improving the resource efficiency and performance of machine learning models. Following are some research projects that I find intriguing.

Professor Hannaneh Hajishirzi and their team create a framework, DECKARD, that involves using a language model (LM) and an RL agent learning the rules of an environment. The LM will formulate a plan for the RL agent to execute, the outcome of which can be used to update the LM's plan in the next cycle. I would love to build on this project by executing only a few subgoals that are most "confusing" for the LM. We can create multiple subgoals and try to estimate the outcome. We will execute the plan only if the system is not confident in its prediction. An interesting challenge would be to quantify uncertainty in such a framework.

Professor Maya Cakmak and their team conduct a study on the shortcomings of a feeding assistant robot in social situations. For example, in a crowded area, the robot cannot hear the user's instruction to feed them because there is background noise. I'm interested in extending this work to use RLHF by building a system that can understand the rules of a social context, using the help of humans (who understand social rules). For example, if an area has background noise, the system will learn that it must increase the sensitivity of its microphone to be able to hear the user. In such a setting, active learning could be useful to improve generalizability.

Professor Noah Smith and their team show that LLMs suffer from hallucination snowballing – if one wrong claim is made, the rest of the answer will be based on the wrong claim. The final answer could be completely off the mark. I'd like to further this work by figuring out ways to create a discriminator component within the chat bot. The discriminator component will evaluate each sentence for factual correctness and confidence of the prediction. It can be trained using human feedback, and will predict without it.

Future Plans. My goal is to continue in academia as a professor where I can explore new related research domains and advise the next generation of researchers. I hope to provide the same excellent guidance that my advisors, mentors, and colleagues have provided me. The Paul G. Allen School of Computer Science at the University of Washington offers an ideal environment for me to conduct the research I am passionate about and hone my teaching and advising skills.

References

Xiong, Z., Agarwal, I., & Jagannathan, S. (2022). Hisarl: A hierarchical framework for safe reinforcement learning. In *Safeai@ aaai*.